



PLANO DE GERENCIAMENTO DE RISCOS DA ETICE

Junho/2021

Presidente da Etice: Lassance de Castro
Diretor do EGC: Marcos Helano Martins Carneiro

EQUIPE DE ELABORAÇÃO:

Regina Estela Benevides de Lima – Gerente do Projeto

Kátia Arruda – Técnica Responsável

Membros - Grupo de Trabalho:

Ana Lucia Pereira Gomes

Francisco Hoilton Araripe Rios

João Alcides Guerra

João José Vasco Peixoto Furtado

Lúcia Pompeu de Vasconcelos Castro

Paulo Henrique Aguiar

Rossana Maria Guerra Luduena

SUMÁRIO

CAPÍTULO I – CONTEXTUALIZAÇÃO

1.1 Introdução

1.1.1. Objetivos

1.1.2. Implantação

1.2. Empresa de Tecnologia da Informação do Ceará – Etice

CAPÍTULO II – ESTRATÉGIAS DE IMPLEMENTAÇÃO

2.1. Estrutura da Gestão de Riscos

2.2. Seleção de Processos

2.3. Identificação dos Responsáveis pelo Processo

2.4. Definição dos Níveis de Apetite ao Riscos

2.5. Estimativas para Execução do Plano

2.6. Preparação da Etice para Implementação do Plano

2.7. Sistemática de Monitoramento e Controle da Implementação do Plano

CAPÍTULO III – METODOLOGIA

3.1. Comunicação e consulta

3.2. Entendimento do contexto

3.3. Processo de Avaliação dos Riscos

3.3.1. Identificação de riscos

3.3.2. Análise de riscos

3.3.3. Avaliação de riscos

3.4. Tratamento de riscos

3.5. Monitoramento e análise crítica

3.6. Registro e relato

3.6.1. Registro

3.6.2. Relato

CAPÍTULO IV – CONSIDERAÇÃO FINAL

CAPÍTULO V – REFERÊNCIAS

CAPÍTULO VI – GLOSSÁRIO

CAPÍTULO VII – ANEXOS

CAPÍTULO I – CONTEXTUALIZAÇÃO

1.1. INTRODUÇÃO

Em qualquer contexto organizacional, independentemente do tipo de negócio, eventos de riscos, externos ou internos à organização, podem ocorrer de forma imprevista. A magnitude e frequência com que isso ocorre caracteriza os riscos que uma organização corre e que podem impedi-la de realizar sua missão de forma adequada. Gerenciar os riscos envolve identificá-los e medi-los para que ações preventivas e corretivas sejam planejadas e desenvolvidas. Visa-se assim mitigar os efeitos negativos que porventura possam advir da ocorrência dos eventos de risco.

No setor público, a gestão de riscos é requisito essencial para a saúde financeira das instituições, proteção do bem público e, em última instância, manter a qualidade do atendimento ao cidadão. Em virtude das Tecnologias da Informação e Comunicação (TIC) estarem presentes em todos os locais e situações, além do fato de que a Etice, como empresa estadual de TIC, é prestadora de serviços essenciais ao pleno funcionamento dos três Poderes no Estado, um plano de gerenciamento de riscos para a Etice se faz necessário.

Tal plano se mostra ainda mais importante diante das recentes mudanças que a Etice vem passando. Além do papel de assessoramento aos órgãos e entidades estaduais em diretrizes, estratégias, políticas, normas, padrões e orientações para o uso de TIC, a empresa passou a ser focada no mercado e na gestão de seus clientes e parceiros, disponibilizando serviços diferenciados, inovadores e competitivos como os serviços de Telecomunicações em banda larga, por meio do Cinturão Digital do Ceará – CDC; o *Voice Over IP* – VoIP, o Videomonitoramento, a Videoconferência e, mais recentemente, o Serviço de Nuvem Computacional. Para isso, tem como parceiros de negócios, grandes provedores de serviços de Nuvem Computacional como Amazon, IBM, Microsoft, Mandic e Oracle.

Este **Plano de Gerenciamento de Riscos (PGR)** especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos na Etice. Em último termo, os colaboradores da empresa poderão assim evitar perdas, além de melhor qualificar a prestação dos serviços públicos.

1.1.1. OBJETIVOS

O Plano de Gerenciamento de Riscos (PGR) da Etice está alinhado à Política Estadual de Gestão de Riscos (Decreto Nº33.805, 09 de novembro de 2020) e à Metodologia de Gerenciamento de Riscos do Poder Executivo do Governo do Estado do Ceará (Portaria CGE Nº 05/2021, 03 de fevereiro de 2021), tendo como principal objetivo dar suporte à governança corporativa e aprimorar o controle interno através das seguintes ações:

a) fortalecer as decisões em resposta aos riscos, a fim de permitir identificar e selecionar alternativas de respostas, tais como: evitar, reduzir, compartilhar e aceitar os riscos;

b) reduzir as surpresas e prejuízos operacionais, fazendo com que a administração adquira melhor capacidade para identificar riscos em potencial e estabelecer respostas a eles, reduzindo surpresas e custos/prejuízos associados;

c) aproveitar oportunidades, onde todos os riscos serão considerados em potencial, de modo que a Etice possa se posicionar para identificar e aproveitar as oportunidades de forma proativa.

Esses elementos auxiliarão os gestores a atingir as metas de desempenho da Etice, a evitar perdas, a melhorar o aproveitamento dos recursos, a prestação de serviços e a entrega de produtos mais seguros e eficientes.

1.1.2. IMPLANTAÇÃO

A estratégia de implementação do PGR da Etice foi pensada em dois momentos a serem feitos em sequência. O primeiro momento refere-se às ações de preparação da organização para que o PGR possa ser implantado. Essa preparação se dá inicialmente no nível estratégico e, em alguns momentos no nível tático. Essas instruções foram criadas para apoiar a alta administração da empresa na definição da estrutura de gerenciamento de riscos, elencando as decisões estratégicas que precisam ser tomadas e os responsáveis por cada uma delas. A competência do Escritório de Governança Corporativa (EGC) para realizar a coordenação das ações de riscos, bem como o mesmo dialoga com as diferentes áreas da organização e com seu Comitê Executivo (composto por seus diretores e presidência), são exemplos de definições que precisam ser adotadas com base nessas instruções. A seleção dos processos a serem priorizados, as estratégias de comunicação e a forma de monitoramento do PGR nos níveis estratégico, tático e operacional, também devem seguir essas instruções.

O segundo momento para implantação do PGR da Etice envolverá, principalmente, seus colaboradores do nível operacional. Definiu-se, então, uma **Metodologia de Gerenciamento de Riscos**, a fim de apoiar na identificação, caracterização e análise dos riscos de cada área de atuação da empresa, bem como orientar nas ações de mitigação e tratamento dos mesmos. Por fim, a metodologia detalha como o processo de documentação e registro de todas as etapas da metodologia deve ser feito.

Este plano oferece também alguns **Formulários Consolidados (Anexo 7.2)** que devem ser usados pelos colaboradores responsáveis pelos processos priorizados. Dessa forma, o PGR pode se desenvolver de forma paralela, com diferentes atividades sendo abordadas, mas todas seguindo as etapas recomendadas pelo plano, de acordo com a realidade da empresa e usando os formulários padrões.

1.2. Empresa de Tecnologia da Informação do Ceará (Etice)

A Etice é uma empresa pública, dotada de personalidade jurídica de direito privado, da Administração Indireta, vinculada à Secretaria do Planejamento e Gestão (Seplag), constituída para fortalecer a gestão pública e o desenvolvimento econômico e social do Estado do Ceará por meio de serviços de Tecnologia da Informação e Comunicação – TIC, atuando em uma área de negócios estratégica de forte indução à inovação e modernização da gestão pública.

Conforme a Lei Nº 16.710 de 21 de dezembro de 2018, que altera a Estrutura da Administração Estadual, a Etice deve assessorar o órgão competente na Administração Pública Estadual na proposição e execução das diretrizes, estratégias, políticas, normas, padrões e orientações para o uso de TIC, a serem observadas pelos órgãos e entidades estaduais.

Atualmente, a Etice persegue uma significativa mudança de estratégia e atuação comercial, passando a ser uma empresa muito mais focada no mercado e na gestão de seus clientes e parceiros, disponibilizando serviços diferenciados, inovadores e competitivos.

A empresa oferta aos seus clientes, por meio do seu Market Place, mais de 200 serviços relacionados aos serviços de Telecomunicações em banda larga, por meio do Cinturão Digital do Ceará – CDC; *Voice Over IP* – VoIP, Videomonitoramento, Videoconferência e, mais recentemente, o Serviço de Nuvem Computacional.

É importante ressaltar que, com a Lei 16.727 de 26/12/2018, Lei do Hub (HTIC), formalizou-se a necessidade de otimizar, de forma contínua, os recursos de custeio e investimentos em TIC, compartilhar recursos de TIC entre os órgãos/entidades da administração, prover novas tecnologias para atender às demandas requeridas pelo serviço público, disponibilizar links de dados e internet de alta velocidade, com qualidade, às unidades administrativas e à população do Estado e fomentar o crescimento econômico no segmento de TIC dentro do Estado, cabendo à Etice, com exclusividade, a responsabilidade de execução destes serviços.

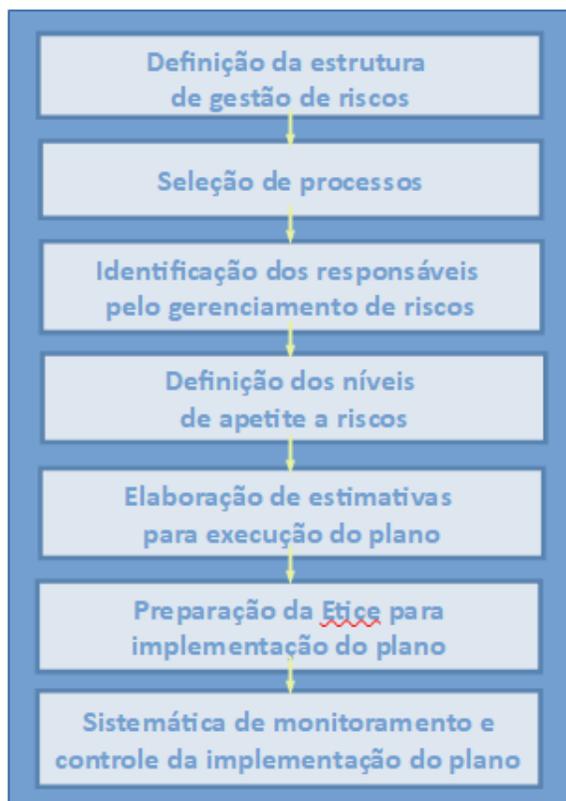
Outra importante Lei é a de nº 13.303/2016 – Lei das Estatais, que estabelece que todas as Empresas devem adotar regras de estruturas e práticas de gestão de riscos para subsidiar seus administradores.

Diante deste cenário, a Gestão de Riscos passou a ser um fator de vital importância para mitigar os impactos oriundos dos novos desafios de TIC, que devem ser previstos, mensurados e monitorados.

CAPÍTULO II – ESTRATÉGIAS DE IMPLEMENTAÇÃO

Este capítulo se propõe a ser um guia para a alta gestão da Etice desenvolver atividades que assegurem a aplicação do processo de gerenciamento de riscos, em todos os níveis e funções pertinentes, como parte de suas práticas e processos.

Essas atividades, divididas nas seguintes etapas, constituem as estratégias para implementação do Plano de Gerenciamento de Riscos, que precedem e preparam a Etice para a aplicação da gestão de riscos, inicialmente, nos processos prioritizados.



2.1. Definição da estrutura de gestão de riscos

A Etice deve implementar e melhorar continuamente a seguinte estrutura com a finalidade de integrar as atividades do processo de gestão de riscos, de forma a auxiliar na eficácia desse gerenciamento, a assegurar que as informações sobre riscos sejam adequadamente reportadas, tratadas e sirvam de base para a tomada de decisões e a responsabilização em todos os níveis aplicáveis da organização.



O gerenciamento de riscos da Etice envolve, portanto, todas as áreas de atuação:

- **estratégica**, representada pelo Comitê Executivo (diretoria e presidência);
- **tática**, através do Escritório de Governança Corporativa (EGC); e
- **operacional**, que contempla os (co)responsáveis pelos processos organizacionais e seus colaboradores.

A área de **Atuação Estratégica** deverá:

- definir as estratégias de implementação do gerenciamento de riscos, considerando os contextos externo e interno;
- avaliar os riscos e a eficácia dos controles internos existentes, em relação aos objetivos dos processos organizacionais selecionados;
- avaliar e validar o resultado do processo de gerenciamento de riscos de cada processo organizacional selecionado;
- avaliar a efetividade das medidas de tratamento e controle implementadas nos processos;
- validar o desempenho do processo de gerenciamento de riscos e o fortalecimento da aderência dos processos organizacionais à conformidade normativa; e
- supervisionar a atuação das áreas quanto ao gerenciamento de riscos.

Além disso, a área de atuação estratégica deve ser **informada** pelas áreas competentes sobre:

- quem são os responsáveis pelos processos selecionados;
- qual o entendimento do contexto em relação ao processo;
- quais os riscos identificados nos processos;
- qual o resultado da análise e avaliação dos riscos (cálculo do risco inerente, classificação do risco residual);
- a implementação do Plano de Tratamento e seu monitoramento;
- a realização da análise crítica dos níveis de riscos e da efetividade do Plano de Tratamento;
- a documentação e relato de cada etapa do gerenciamento de riscos do processo – Registro e Relato.

A área de atuação estratégica, também, deve **aprovar**:

- a seleção dos processos críticos realizada pelos gestores das áreas;
- os níveis de apetite a riscos dos processos;
- os indicadores de desempenho para a gestão de riscos, alinhados com os indicadores de desempenho da Etice;
- a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
- a identificação dos riscos que serão priorizados para tratamento;

- o Plano de Tratamento (definição das respostas aos riscos e as medidas de tratamento e controle) a ser implementado nos processos organizacionais; e
- o Plano de Comunicação e Consulta de Gerenciamento de Riscos.

Quanto à área de **Atuação Tática**, suas funções compreendem:

- auxiliar na identificação dos objetivos da organização e na compreensão dos contextos externo e interno a serem considerados no gerenciamento de riscos;
- auxiliar na identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação do gerenciamento de riscos;
- auxiliar na definição das respostas aos riscos e das medidas de tratamento e controle a serem implementadas nos processos organizacionais (Plano de Tratamento);
- auxiliar na definição dos indicadores de desempenho para a gestão de riscos, alinhados com os indicadores de desempenho da Etice;
- propor o plano de comunicação e consulta de gerenciamento de riscos;
- propor a atualização das estratégias de gerenciamento de riscos, considerando os contextos externo e interno;
- propor a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
- realizar o monitoramento e a análise crítica dos níveis de riscos e da efetividade das medidas de tratamento e controle implementadas nos processos organizacionais;
- auxiliar na definição dos níveis de apetite a riscos dos processos organizacionais, caso sejam diferentes dos propostos na Metodologia de Gerenciamento de Riscos do Poder Executivo Estadual;
- auxiliar na identificação dos responsáveis pelo gerenciamento de riscos dos processos organizacionais;
- avaliar os indicadores de desempenho para a gestão de riscos objetivando melhoria contínua;
- requisitar aos responsáveis as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais;
- acompanhar o desempenho do processo de gerenciamento de riscos e estimular o fortalecimento da aderência dos processos críticos à conformidade normativa;
- documentar e informar as outras áreas de atuação cada etapa do processo de gerenciamento de riscos.

Em relação à área de **Atuação Operacional**, suas funções compreendem:

- identificar os objetivos da organização e compreender os contextos externo e interno a serem considerados na gestão de riscos;
- identificar, analisar e avaliar os riscos dos processos organizacionais selecionados para a implementação do gerenciamento de riscos;

- definir os níveis de apetite a risco dos processos organizacionais, caso sejam diferentes dos propostos na Metodologia de Gerenciamento de Riscos do Poder Executivo Estadual;
- propor as respostas aos riscos e as medidas de tratamento e controle a serem implementadas nos processos organizacionais (Plano de Tratamento);
- monitorar os níveis de riscos e a efetividade das medidas de tratamento e controle implementadas nos processos organizacionais sob sua responsabilidade;
- informar à área de atuação tática sobre mudanças significativas nos processos organizacionais sob sua responsabilidade;
- propor os indicadores de desempenho para a gestão de riscos, alinhados com os indicadores de desempenho da Etice;
- responder às requisições da área de atuação tática;
- disponibilizar as informações quanto ao gerenciamento de riscos dos processos sob sua responsabilidade a todos os níveis da organização e demais partes interessadas;
- realizar outras atividades de gerenciamento de riscos dos processos sob sua responsabilidade, em conformidade com a Política de Gestão de Riscos do Poder Executivo Estadual.

Essas áreas de atuação devem ser definidas por meio de Portaria e manter fluxo regular e constante de comunicação.

2.2. Seleção de Processos

Nesta etapa, os processos organizacionais que serão objeto do processo de gerenciamento de riscos deverão ser selecionados **pelos gestores das áreas, com o auxílio da área de atuação operacional e sob a coordenação da Área de Atuação Tática**, preferencialmente dentre os processos mais críticos, sendo documentadas as justificativas e informações sobre os aspectos e eventos considerados na sua escolha.

Para a realização desta seleção, serão analisados aspectos tais como: relevância do processo para missão, metas, objetivos estratégicos, imagem e credibilidade da Etice junto a seus *stakeholders*, volume de recursos orçamentários e financeiros aplicados, aquisições diretas de bens e serviços, impacto na capacidade da Etice de realizar suas atividades com qualidade, tempestividade e continuidade operacional, bem como adequação das legislações, normativos, liderança, planos, sistemas, infraestrutura e pessoas, dentre outros. A seleção dos processos organizacionais deverá ser submetida à aprovação da área de **Atuação Estratégica**.

2.3. Identificação dos Responsáveis pelo Processo

Para cada processo organizacional selecionado deverá ser identificado um responsável pelo gerenciamento de riscos do processo, dentre as lideranças das diversas áreas que executam a maior parte de suas atividades ou as mais relevantes.

O processo de gerenciamento de riscos envolve diversas áreas de atuação, gestores e colaboradores, devendo todos terem conhecimento sobre suas funções e responsabilidades, conforme definidas no **Anexo 7.1 - Matriz de Responsabilidades (RACI)** e de acordo com quadro a seguir:

QUADRO 1: Funções e Responsabilidades

Funções	Responsabilidades
Controle Interno e gestores de cada área	<p>Certificar que os riscos foram identificados e tratados de modo a aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no processo.</p> <p>Monitorar os riscos.</p> <p>Divulgar informações pertinentes aos riscos do processo.</p>
Ouvidoria	<p>Receber manifestações acerca do gerenciamento de riscos e encaminhar para o responsável da área tática e demais áreas competentes.</p>
Comunicação	<p>Realizar atividades para assegurar que os responsáveis pela implementação do PGR da Etice e todas as partes interessadas compreendam os fundamentos sobre os quais as decisões serão tomadas e as razões pelas quais ações específicas serão requeridas.</p>
Projur	<p>Assessorar juridicamente os envolvidos no processo de gerenciamento de riscos em relação às decisões contratuais relacionadas aos riscos.</p>
Comitê Executivo (Presidência, Diretoria e Projur)	<p>Aprovar o plano de gerenciamento de riscos e suas reservas de contingências.</p> <p>Aprovar o uso das reservas de contingência.</p>
Presidente da Etice	<p>Garantir o apoio institucional para promover a gestão de riscos, em especial, os recursos necessários, o relacionamento entre as partes interessadas e o desenvolvimento contínuo das pessoas e dos processos, em observância ao Programa de Integridade do Poder Executivo do Governo do Ceará.</p>
Gestores de cada área	<p>Identificar os processos organizacionais mais críticos que impactam diretamente no atingimento dos objetivos estratégicos do órgão que comporão o gerenciamento de riscos, bem como os responsáveis por esses processos, para ser implementado de forma gradual;</p> <p>Monitorar o gerenciamento dos riscos dos processos sob a responsabilidade da sua área.</p>
Responsáveis por gerenciar os riscos do processo priorizado	<p>Aplicar a metodologia de gerenciamento de riscos no processo sob sua responsabilidade.</p>
Colaboradores da Etice	<p>Comunicar a situação dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.</p> <p>Reportar imediatamente ao responsável pelo gerenciamento de riscos do processo em questão, que reportará o fato à instância de atuação tática do órgão, caso sejam identificadas mudanças ou fragilidades nos processos organizacionais.</p>

2.4. Definição dos Níveis de Apetite ao Risco

A área de atuação estratégica da Etice deverá produzir um documento (declaração) com os níveis de Apetite ao Risco, contendo claros limites de tolerância e um modelo financeiro que suporte os riscos para subsidiar a implementação do plano de gerenciamento de riscos nos processos organizacionais selecionados, orientar o comportamento da empresa e as tomadas de decisões estratégicas. Assim, a Etice deverá estabelecer um entendimento comum dos riscos, determinar quais riscos está disposta a tolerar e qual a quantidade de risco que precisará ser gerenciada, assim estará preparada para a probabilidade e os impactos das ameaças conhecidas.

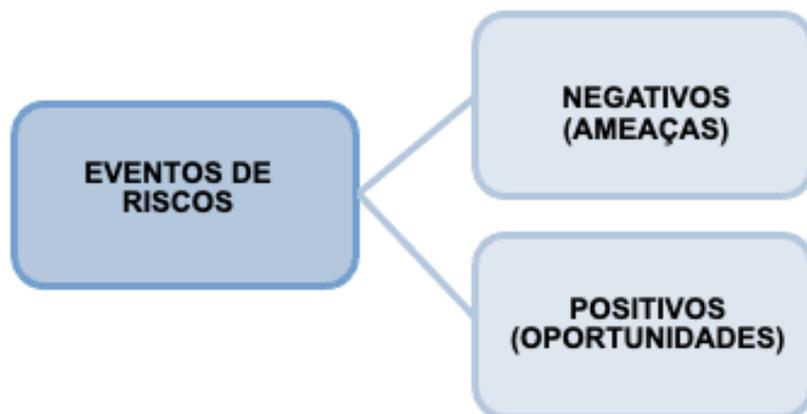
Para isso, é necessário que se tenha um entendimento dos valores corporativos e da cultura de risco, antes de iniciar o processo de identificação dos níveis de Apetite ao Risco, alinhados com a estratégia da organização e com as perspectivas das partes interessadas.

Então, deve-se entender qual a estratégia, as metas, as expectativas dos *stakeholders* e a cultura da Etice quanto aos riscos, para analisar os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados, tais como pessoas, sistemas informatizados, estruturas organizacionais, legislações, recursos, dentre outros.

Para desenvolver um Apetite ao Risco, deve-se refletir sobre quais os riscos inerentes à estratégia, quantos e quais tipos de riscos, os *stakeholders* podem assumir, bem como analisar dentre outros itens, o perfil e a capacidade de risco.

Compreende-se por perfil de risco, os principais riscos da organização e os controles para mitigá-los e por capacidade de risco, o quanto de risco a organização pode absorver. Para facilitar as análises, os riscos devem ser classificados em categorias de ameaças/oportunidades relacionadas com o negócio da Etice e seus processos organizacionais.

Entende-se eventos de riscos, como situações em potencial que ainda não ocorreram, que podem causar impacto na consecução dos objetivos estratégicos da organização, caso venham a ocorrer. Os eventos de riscos negativos são denominados ameaças com consequências negativas, levando a prejuízos para a organização, enquanto os riscos positivos são eventos que geram oportunidades com consequências positivas, e costumam gerar benefícios, melhorias ou ganhos para a organização.



A categorização dos riscos corporativos é outro aspecto importante para auxiliar na análise dos riscos e deve estar relacionada com o que a Etice faz, envolvendo, portanto, as seguintes categorias de riscos, que são as mais comuns, relacionadas ao seu tipo de negócio:

a) Riscos estratégicos: eventos que podem impactar na missão, nas metas ou nos objetivos estratégicos da Etice, caso venham a ocorrer;

b) Riscos de imagem: eventos que podem comprometer a credibilidade da Etice junto ao público externo e interno, causado por má interpretação ou falha na comunicação; por divulgação de informações incorretas, incompletas ou imprecisas, por pessoas não autorizadas ou por meios de comunicação inadequados e por veiculação de notícias negativas sobre a empresa e seus serviços;

c) Riscos de corrupção: eventos que podem envolver compras diretas de produtos ou serviços para a Etice, com o emprego de recursos financeiros significativos; atribuição de direitos ou benefícios ao público – que são processos em que a administração pública pode reconhecer situações que concedam direitos a cidadãos ou empresas, como a emissão de certificados, concessões, dentre outros: transferência de recursos entre organizações públicas dos diversos níveis de governo ou entre a administração pública e entes privados; a verificação do cumprimento de obrigações e a aplicação de penalidades;

d) Riscos financeiros/orçamentários: eventos que podem comprometer a capacidade da Etice de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou, ainda, eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;

e) Riscos de conformidade: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da Etice;

f) Riscos operacionais/pessoais: eventos que podem comprometer as atividades da Etice, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, contratos, infraestrutura e sistemas;

g) Tecnológicos: representados por ameaças ou oportunidades relacionadas a hardware e software;

h) Ambientais: associados às questões de meio ambiente e à redução de seus impactos.

É importante ressaltar, que o método para identificação do apetite a riscos, definido na metodologia de gerenciamento de riscos para os processos organizacionais, deve ser aplicado também nesta etapa de estratégias de implementação. Além disso, vale destacar também que não faz sentido gastar recursos para gerenciar riscos que não possuam tanta relevância para o negócio em si e para os seus *stakeholders*. Portanto, os custos devem ser também levados em consideração nesse processo.

2.5. Estimativas para execução do plano

Nesta etapa, devem ser realizadas as estimativas de orçamento e tempo para assegurar que a Etice disponha de recursos orçamentários e financeiros suficientes para o desenvolvimento da gestão de riscos, nos processos organizacionais selecionados, e que o cronograma das atividades façam parte do planejamento da Etice.

Para isso, a área responsável pela realização das atividades de gerenciamento de riscos no processo organizacional selecionado, deve propor os prazos, elaborando o cronograma e a estimativa dos custos a serem alocados, de acordo com as diretrizes institucionais, para submetê-los à aprovação e ao acompanhamento pelas instâncias competentes.

Por fim, ressalta-se ainda, que deve ser previsto o ciclo de revisão do processo de gerenciamento de riscos para cada processo organizacional, **a cada 2 anos**, ou sempre que houver eventos que coloquem em risco o processo selecionado.

2.6. Preparação da Etice para Implementação do Plano

Uma vez definidos e aprovados, o plano para implementação e a metodologia de gerenciamento de riscos a ser aplicada nos processos organizacionais, é necessário o apoio da alta gestão, no provimento dos recursos necessários e na divulgação da importância e dos benefícios da gestão de riscos para o alcance dos objetivos da Etice e seu desenvolvimento institucional.

Por tratar-se de um processo novo, é importante sensibilizar, capacitar e envolver a maior quantidade de pessoas da Etice no desenvolvimento de uma cultura de gestão de riscos, criando oportunidades para troca de experiências, divulgação de conceitos, boas práticas e técnicas relacionados com gerenciamento de riscos.

Para o sucesso da gestão de riscos na Etice, o processo de gerenciamento de riscos deve ser incorporado aos processos organizacionais e deve ser utilizada uma comunicação multidirecional, de tal forma que possam ser tomadas decisões a partir de informações adequadas, tempestivas, corretas, atuais e de fácil acesso, sobre o nível de riscos e sobre a necessidade de tratamento, de acordo com o perfil de risco institucional, reduzindo as chances de que a alta administração só tome ciência de um risco após se transformar em crise.

2.7. Sistemática de Monitoramento e Controle da Implementação do Plano

A implementação do plano de gerenciamento de riscos deve ser monitorada regularmente pela área de atuação tática e operacional, pelo gestor da área e o gestor responsável pelo gerenciamento de riscos, mantendo informados os colaboradores e a área de atuação estratégica.

O monitoramento e a análise crítica devem ser planejados como parte do processo de gestão de riscos, realizados periodicamente e utilizados para aferir se as atividades estão sendo realizadas, de acordo com o planejado para cada processo selecionado, seguindo a metodologia estabelecida. Os resultados do monitoramento e a análise crítica devem ser registrados para subsidiar ajustes e melhorias, que podem ser incorporadas na gestão, na mensuração e na apresentação de informações a respeito do desempenho da gestão de riscos.

CAPÍTULO III - METODOLOGIA

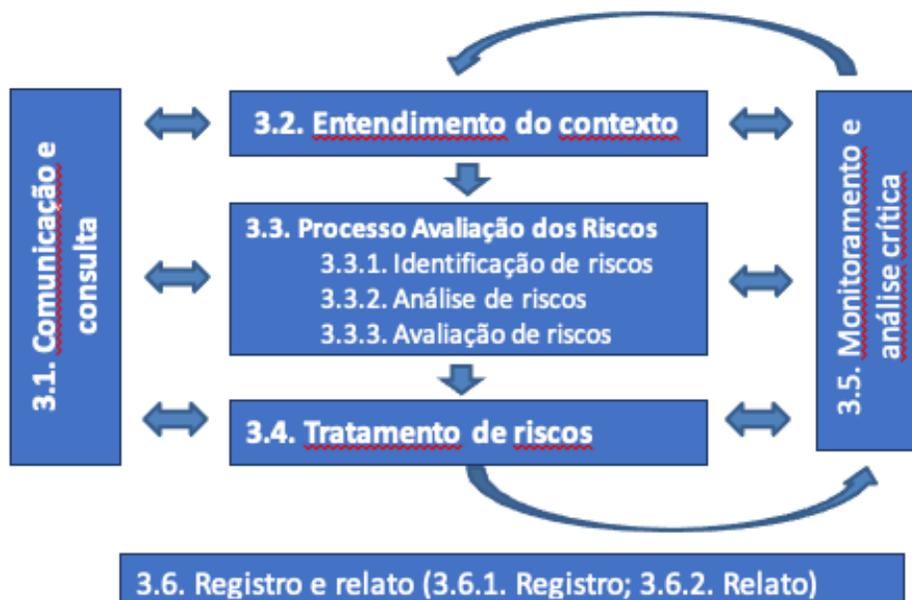
O Plano de Gerenciamento de Riscos (PGR) da Etice, alinhado com a política do Poder Executivo do Ceará, define processos, técnicas e ferramentas seguindo as seguintes etapas:

- Comunicação e consulta
- Entendimento do contexto
- Processo de Avaliação dos riscos
- Identificação de riscos
- Análise de riscos
- Avaliação de riscos
- Tratamento de riscos
- Monitoramento e análise crítica
- Registro e relato

3.1. Comunicação e Consulta

Esta etapa busca assegurar que os responsáveis pela implementação do processo de gerenciamento de riscos e partes interessadas conheçam os **fundamentos** sobre os quais decisões são tomadas e razões pelas quais ações específicas são requeridas. Sua função é de **informar e sensibilizar** todos os envolvidos no processo, estabelecendo e fortalecendo contatos e relacionamentos entre os públicos internos e externos da empresa. Ela permeia, assim, todas as etapas essenciais do processo. Para tanto, é crucial que as áreas de atuação (co)responsáveis mantenham um fluxo regular e constante de comunicação.

INTEGRAÇÃO DA COMUNICAÇÃO E CONSULTA COM DEMAIS FASES DO GERENCIAMENTO DE RISCOS



Ademais, durante as etapas do processo de gerenciamento de riscos da empresa, é importante que a comunicação observe os agentes, ou áreas apontadas, como **consultados (C) ou informados (I)**, como descrito na **Matriz de Responsabilidades – RACI (Anexo 7.1)**.

As informações colhidas por meio da consulta embasam e orientam as partes no processo de tomada de decisão ou de definição da direção a respeito de uma questão específica. Compete à área de atuação tática para gerenciamento de riscos (EGC) propor um plano de comunicação e consulta para gerenciamento de riscos. A aprovação do plano é de responsabilidade da área de atuação estratégica. Para o planejamento e operacionalização da etapa de Comunicação e Consulta, será elaborado no início da implementação do processo de gerenciamento de riscos, um cronograma de atividades, utilizando o modelo sugerido no **Anexo 7.2 (Formulário 1 – Plano de Comunicação e Consulta)**.

Por fim, e para garantir a aferição do progresso obtido, ou o desvio, em relação ao plano de comunicação e consulta, o EGC realizará, periodicamente, o devido monitoramento. O acompanhamento servirá também para uma retroalimentação do processo de gestão de riscos da empresa.

3.2. Entendimento do contexto

No entendimento do contexto, o processo organizacional e seus objetivos são analisados à luz de seus ambientes interno e externo, devendo a **área de atuação operacional, auxiliada pela área de atuação tática**, identificar os itens abaixo:

- Descrição resumida do processo organizacional. A descrição é um breve relato sobre o processo que permite compreender o seu fluxo, a relação entre os atores envolvidos e os resultados esperados;
- Área responsável pelo processo organizacional;
- Ciclo médio do processo organizacional (em dias);
- Sistemas tecnológicos que apoiam o processo organizacional;
- Partes interessadas no processo organizacional, podendo ser internas ou externas;
- Fluxo (mapa) do processo organizacional;
- Objetivos do processo organizacional. É importante apontar quais objetivos são alcançados pelo processo organizacional. Se possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando perspectivas estratégicas, temporais, relacionais, financeiras, orçamentárias, metas, entre outras. Para identificação dos objetivos, pode-se buscar responder à questão “O que deve ser atingido nas diversas dimensões para se concluir que o processo ocorreu com sucesso?”;
- Relação de objetivos estratégicos da organização alcançados pelo processo;

- Justificativa para o gerenciamento de riscos no processo organizacional. Apresentar os motivos que levaram a implementar o gerenciamento de riscos no processo organizacional. A criticidade do processo organizacional que impacta diretamente no atingimento dos objetivos estratégicos pode ser uma das justificativas para gerenciá-lo;
- Leis e regulamentos relacionados ao processo organizacional;
- Informações sobre o contexto externo do processo organizacional, considerando cenário atual ou futuro, oportunidades e ameaças relacionadas, percepções das partes interessadas externas e outros fatos relevantes;
- Informações sobre o contexto interno do processo organizacional, considerando políticas, objetivos, diretrizes e estratégias que o impactam, forças e fraquezas relacionadas, percepções das partes interessadas internas, principais ocorrências de problemas e outros fatos relevantes;
- O ciclo de revisão do processo de gerenciamento de riscos de processos organizacionais **deve ocorrer a cada 2 anos**, ou sempre que houver eventos que coloquem em risco o processo;
- O tratamento de risco se dará com base no apetite a risco determinado pela empresa.

3.3. Processo de Avaliação de Riscos

O processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos, propriamente dita.

3.3.1. Identificação de riscos

Nesta etapa deve-se construir uma lista de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas (eventos de risco ou riscos).

Os riscos ou eventos de riscos podem ser identificados a partir das seguintes perguntas:

- Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?

Em seguida, algumas perguntas podem ser realizadas para garantir a veracidade dos eventos de riscos:

- O evento é um risco que pode comprometer claramente um objetivo do processo organizacional?
- O evento é um risco ou uma falha no desenho do processo organizacional?
- À luz dos objetivos do processo organizacional, o evento identificado é um risco ou uma causa para um risco?
- O evento é um risco ou uma fragilidade em um controle para tratar um risco do processo organizacional?

Identificados os riscos em potencial que, se ocorrerem, afetarão a empresa e podem afetar os processos, eles devem ser documentados com as suas características no **Anexo 7.2 (Formulário 2 – Identificação e Análise de Riscos)**.

3.3.1.1. Origem

Os riscos podem ser:

- Externos: são os riscos associados ao ambiente em que a Etice opera. Em geral, não há governabilidade sobre eles, mas ações podem ser tomadas quando necessário.
- Internos: são os riscos associados à própria estrutura da Etice, seus processos, governança, quadro de pessoal, orçamento ou ambiente de tecnologia. A Etice pode e deve agir pro-ativamente sobre os mesmos.

3.3.1.2. Categorias

As categorias de riscos servem para que os eventos de riscos possam ser classificados e agrupados pelas possíveis causas, de modo a facilitar o seu gerenciamento. Essas categorias refletem diferentes dimensões tais como: ambiental, conformidade, econômico, pessoal, tecnológico, dentre outros, conforme descrito no **subitem 2.4 – Definição dos Níveis de Appetite ao Risco**.

3.3.2. Análise de riscos

A análise de riscos visa promover o entendimento do nível de riscos e de sua natureza, identificar suas possíveis causas, consequências e os controles existentes para prevenir sua ocorrência e diminuir o impacto de suas consequências. Ela pode ser realizada com diversos graus de detalhe, dependendo do risco, da finalidade da análise e das informações, dados e recursos disponíveis. Dependendo das circunstâncias, a análise pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas.

De uma forma geral, os processos mais críticos devem ter seus riscos analisados de forma quantitativa e qualitativa. No entanto, como já mencionado no parágrafo anterior, reconhece-se que a implementação de uma análise quantitativa pode ser complexa, num primeiro momento, dado o nível de maturidade de cada área e a disponibilidade de dados. Entretanto, quando da análise quantitativa, deverão ser calculados os valores monetários esperados para cada risco priorizado.

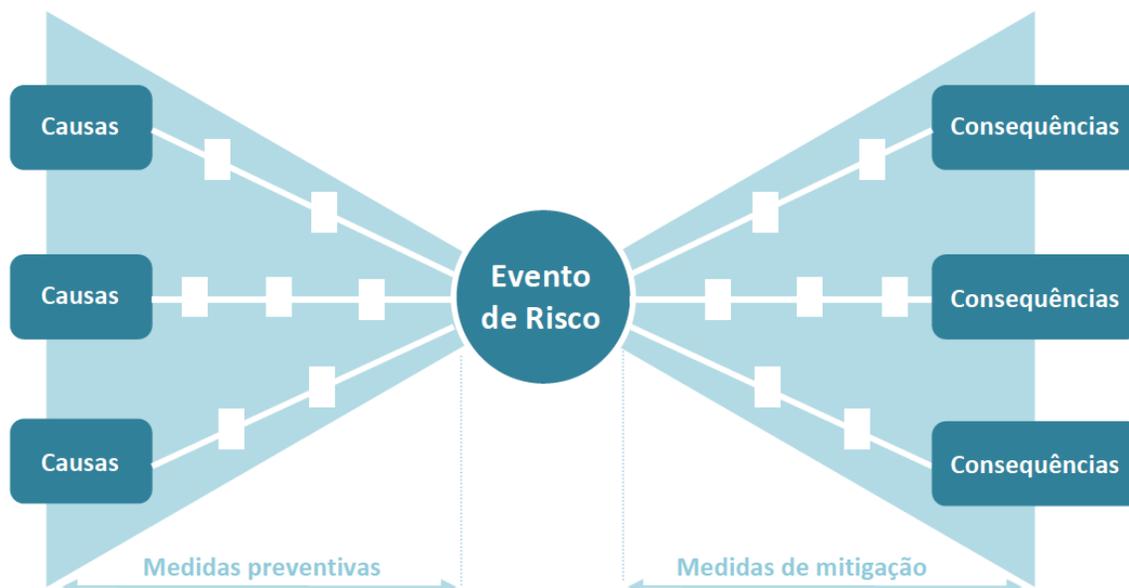
A análise qualitativa de riscos será utilizada na avaliação das exposições dos processos da Etice aos possíveis riscos, para posterior priorização. Aqueles com menor probabilidade e impacto serão mantidos nos registros dos riscos dentro de uma lista de observação para monitoramento futuro.

Para eventos identificados como riscos do processo organizacional, a área de atuação operacional, com auxílio da área de atuação tática, deve indicar:

- Etapa e objetivo do processo organizacional que são impactados pelo risco;
- Categorias dos riscos;
- Causas do risco: motivos que podem promover sua ocorrência;
- Consequências do risco: resultados provocados pelo risco que afetam os objetivos do processo organizacional;
- Controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos/checklist definidos para o processo e capacitação dos servidores envolvidos no processo organizacional, etc.;
- Controles de atenuação e recuperação: controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especial; procedimento apuratório, etc.

A análise de riscos deve ser realizada no início de um novo processo e como parte da gestão contínua dos processos existentes. Normalmente, a análise verifica e compara o nível atual de riscos com os controles existentes. Para os riscos mais severos, na medida do possível, uma análise quantitativa deve ser realizada considerando sua probabilidade e seu impacto. As informações produzidas nas etapas de Identificação e Análise de Riscos devem ser registradas no **Anexo 7.2 (Formulário 2 – Identificação e Análise de Riscos)**.

Os potenciais riscos podem ser organizados através de uma Estrutura Analítica dos Riscos – EAR (com representação hierárquica dos riscos), de acordo com suas categorias. O método mais indicado é o “bow-tie” (gravata-borboleta), como representado a seguir:



3.3.3. Avaliação de riscos

A finalidade da Avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados da etapa de análise de riscos (subitem 3.3.2 acima), sobre quais riscos necessitam de tratamento, bem como as prioridades na implementação do tratamento. Nesta etapa, a **área de atuação operacional, com auxílio das áreas de atuação tática e estratégica** deverão

- Calcular o **Risco Inerente (RI)**, a partir de critérios de probabilidade e impacto, como apresentadas nos Quadros 2 e 3, de acordo com sua complexidade, a seguir:

QUADRO 2: ESCALA DE PROBABILIDADE		
PROBABILIDADE	DESCRIÇÃO DA PROBABILIDADE (desconsiderando os controles)	PESO (NP)
MUITO BAIXA	Improável – Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
BAIXA	Rara – De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
MÉDIA	Possível – De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
ALTA	Provável – De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
MUITO ALTA	Praticamente certa – De forma, inequívoca, o evento ocorrerá pois, as circunstâncias indicam claramente essa possibilidade.	10

QUADRO 3: ESCALA DE IMPACTO		
IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS (estratégicos, operacionais, de informação/ comunicação/ divulgação ou de conformidade) DO PROCESSO ORGANIZACIONAL, caso o evento ocorra	PESO (NI)
MUITO BAIXO	Mínimo impacto nos objetivos do processo organizacional.	1
BAIXO	Pequeno impacto nos objetivos do processo organizacional.	2
MÉDIO	Moderado impacto nos objetivos do processo organizacional, porém recuperável.	5
ALTO	Significativo impacto nos objetivos do processo organizacional, de difícil reversão.	8
MUITO ALTO	Catastrófico impacto nos objetivos do processo organizacional, de forma irreversível.	10

- Classificar o risco dentro das faixas apresentadas no quadro a seguir:

QUADRO 4: CLASSIFICAÇÃO DOS RISCOS	
CLASSIFICAÇÃO	FAIXA
Risco Baixo – RB	0 – 9,99
Risco Médio – RM	10 – 39,99
Risco Alto – RA	40 – 79,99
Risco Extremo – RE	80 – 100

- Avaliar a eficácia dos controles internos existentes, em relação aos objetivos do processo organizacional, de acordo com o quadro, a seguir:

QUADRO 5: NÍVEIS DE AVALIAÇÃO DOS CONTROLES INTERNOS EXISTENTES		
NÍVEL DE EFICÁCIA DOS CONTROLES INTERNOS	DESCRIÇÃO	FATOR DE AVALIAÇÃO DOS CONTROLES(FC)
INEXISTENTE	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
FRACO	Controles têm abordagens <i>ad hoc</i> , tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
MEDIANO	Controles implementados, mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
SATISFATÓRIO	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
FORTE	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	0,2

Os riscos com maior probabilidade e impacto deverão ser priorizados para criação de um plano de tratamento e respostas. Aqueles com menor probabilidade e impacto serão mantidos nos registros dos riscos dentro de uma lista de observação para monitoramento futuro. (Risco residual é o risco restante ao qual uma organização está exposta, mesmo após a implementação de medidas de controle para o tratamento dos riscos mais críticos.)

O nível de risco será avaliado em função do seu **Impacto e Probabilidade**, com amplitude em quatro níveis (risco extremo, alto, moderado e baixo), definida em uma matriz cinco por cinco. Podemos calculá-lo com a seguinte equação:

NÍVEL DE RISCO = IMPACTO x PROBABILIDADE
 (NR = NI x NP)
 O NÍVEL DE RISCO é o resultado da multiplicação do IMPACTO pela PROBABILIDADE.

A **Matriz de Riscos** abaixo apresenta os possíveis resultados da combinação das escalas de probabilidade e impacto, assim:

QUADRO 6: MATRIZ DE RISCOS – IMPACTO x PROBABILIDADE						
IMPACTO	MUITO ALTO 10	10 RM	20 RM	50 RA	80 RE	100 RE
	ALTO 8	8 RB	16 RM	40 RA	64 RA	80 RE
	MÉDIO 5	5 RB	10 RM	25 RM	40 RA	50 RA
	BAIXO 2	2 RB	4 RB	10 RM	16 RM	20 RM
	MUITO BAIXO 1	1 RB	2 RB	5 RB	8 RB	10 RM
	MUITO BAIXA 1	BAIXA 2	MÉDIA 5	ALTA 8	MUITO ALTA 10	
	PROBABILIDADE					

Risco Extremo – RE; Risco Alto – RA; Risco Médio – RM; Risco Baixo – RB

3.3.3.1. Cálculo do Risco Inerente

Risco Inerente é o risco a que uma organização está exposta, sem considerar quaisquer medidas de controle que reduzam ou possam reduzir a probabilidade de sua ocorrência ou de seu impacto.

A multiplicação entre os pesos atribuídos a cada escala de probabilidade (Quadro 2) e de impacto (Quadro 3) definirá o nível do **Risco inerente (RI)**:

$$RI = NP \times NI$$

Onde:

RI = nível do risco inerente

NP = Peso da escala de probabilidade (Quadro 3: ESCALA DE PROBABILIDADE)

NI = Peso da escala de Impacto (Quadro 4: ESCALA DE IMPACTO)

Após a classificação do risco, conforme descrito no Quadro 5, a área de atuação estratégica deve avaliar a eficácia dos controles internos existentes, em relação aos objetivos do processo organizacional. Para isso, é necessário verificar se os controles apontados durante a etapa de **Análise dos Riscos (subitem 3.3.2)** auxiliam no tratamento adequado desses riscos.

3.3.3.2. Cálculo de Risco Residual

Após a avaliação dos controles existentes, conforme Quadro 5 (acima), a área de atuação operacional deverá também calcular riscos residuais.

O **Risco Residual – RR** é o risco restante a que uma organização está exposta mesmo após a implementação de medidas de controle para o tratamento do risco. O nível de risco residual corresponde ao valor final da multiplicação entre o valor do risco inerente e o fator de avaliação dos controles internos existentes:

$$RR = RI \times FC$$

Onde:

RR = risco residual

RI = risco inerente

FC = fator de avaliação dos controles existentes

As informações produzidas nesta etapa de Avaliação dos Riscos podem ser registradas como descrito no modelo disponível no **Anexo 7.2 (Formulário 3 – Avaliação dos Riscos)**, ao final deste documento.

O processo organizacional deve ser revisado em cada novo ciclo do processo de gerenciamento de riscos. De forma geral, nos ciclos seguintes de gerenciamento de riscos do processo organizacional, deve-se considerar o nível de risco inerente calculado no 1º ciclo e reavaliar os controles para o cálculo também de risco residual. A comparação entre

os níveis de riscos residuais de diferentes ciclos objetiva identificar se os controles definidos no **Plano de Tratamento** estão sendo eficazes.

3.4. Tratamento de riscos

O tratamento de riscos envolve a seleção de opções que, uma vez implementadas, modificam os riscos, criam novos controles ou alteram os existentes.

Esse processo compõe as atividades de:

- alinhar o apetite ao risco e a estratégia da empresa;
- priorizar os riscos para tratamento;
- definir respostas aos riscos priorizados;
- definir medidas de Tratamento e Controle;
- elaborar Plano de Tratamento aos eventos de riscos;
- validar o resultado do Processo de Gerenciamento de Riscos e, por fim,
- implementar o Plano de Tratamento aos eventos de riscos.

3.4.1 Alinhamento do apetite ao risco à estratégia da empresa

A administração da empresa deve considerar em primeiro lugar o apetite ao risco, avaliar as opções estratégicas e fixar objetivos compatíveis com a estratégia escolhida, bem como desenvolver mecanismos para administrar os riscos implícitos.

A Matriz de Riscos, com os **Níveis de Apetite, Tolerância e Capacidade aos Riscos**, segundo a figura a seguir, mostra os respectivos níveis de acordo com as seguintes definições:

- Apetite ao Risco: Trata-se de quadrantes cuja criticidade é aceita pela Etice, mediante tratativas estabelecidas pelos gestores para atingir seus objetivos, representado com o numeral **“1”** na matriz abaixo. Deve-se planejar e aprovar planos de ação, preventivos, (visando reduzir a probabilidade) e/ou corretivos (visando reduzir impactos) no prazo máximo de 30 dias;
- Tolerância a Risco: Trata-se de quadrantes cuja criticidade está além do apetite ao risco, desta forma, o risco não é aceito pela Etice, representado como numeral **“2”** na matriz abaixo. Deve-se planejar e aprovar planos de ação preventivos (visando reduzir a probabilidade) e/ou corretivos (visando reduzir impactos) no prazo máximo de 15 dias;
- Capacidade de Risco: Trata-se de quadrantes cuja criticidade é extrema, demandando ações imediatas, representado com o numeral **“3”** na matriz abaixo. Deve-se planejar e aprovar planos de ação preventivos (visando reduzir a probabilidade) e/ou corretivos (visando reduzir impactos) imediatamente.

MATRIZ DE RISCOS COM OS NÍVEIS DE APETITE, TOLERÂNCIA E CAPACIDADE AOS RISCOS

		Impacto				
		Muito Leve	Leve	Moderado	Severo	Massivo
Probabilidade	Elevada	1	1	2	3	3
	Muito Alta	1	1	1	2	3
	Alta	1	1	1	2	2
	Média	1	1	1	1	1
	Baixa	1	1	1	1	1

A **Capacidade de Risco** foi definida levando-se em consideração riscos cujos impactos são massivos ou severos e probabilidade de concretização elevada, sendo assim, tratam-se de riscos que, no ambiente de estudo, devem ser tratados prioritariamente haja vista possuírem grande potencial de danos a estratégia da empresa.

A **Tolerância a Risco** foi definida levando-se em consideração riscos com probabilidade considerável de se concretizar, cujo impacto trará danos significativos a estratégia da empresa e, desta forma, devem ser tratados com regime de urgência.

O **Apetite ao Risco** foi definido levando-se em consideração duas premissas: riscos de alta probabilidade de concretização com impacto gerenciável e riscos de baixa probabilidade de concretização com impacto severo ou massivo, demandando, desta forma, ações a médio prazo.

Os demais quadrantes são os riscos cuja probabilidade e impacto podem ser aceitos pela empresa, sendo necessário somente um constante monitoramento deles.

3.4.2. Priorização dos Riscos para Tratamento

Nesta etapa, a área de atuação operacional, com auxílio da área de atuação tática, identificará quais riscos serão priorizados para tratamento. Para isso, devem considerar os valores dos níveis de riscos residuais, calculados no subitem **3.3.3.2 (Cálculo do Risco Residual)**, assim como a faixa de classificação do risco residual. Esta última deve ser considerada para a definição da atitude da área de atuação operacional em relação à priorização para tratamento.

O **Quadro 7** (abaixo) mostra quais ações devem ser adotadas, em relação a cada nível de risco e suas exceções:

QUADRO 7: ATITUDE PERANTE O RISCO PARA CADA CLASSIFICAÇÃO			
FAIXA DE CLASSIFICAÇÃO DE RISCO RESIDUAL	DE DO	AÇÃO NECESSÁRIA	EXCEÇÃO
RISCO BAIXO		Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo responsável pelo processo.
RISCO MÉDIO		Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da área na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo responsável pelo processo.
RISCO ALTO		Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao gestor da área e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do gestor da área em comum acordo com responsável pelo processo.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo responsável pelo processo.
RISCO EXTREMO		Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado à área de atuação estratégica e ao responsável pelo processo e ter uma resposta imediata. Postergação de medidas só com autorização da área de atuação estratégica.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo responsável pelo processo e aprovada pela área de atuação estratégica.

Uma vez definido seu Apetite a Risco, para os processos organizacionais selecionados, a empresa deverá declarar que:

- 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;
- 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.

As informações produzidas nesta etapa devem ser registradas no **Anexo 7.2 (Formulário 4 – Priorização dos Riscos)**, disponível ao final deste documento.

3.4.3. Definição de Respostas aos Riscos

Esta etapa tem como objetivo definir as opções de tratamento para os riscos priorizados, como já descrito acima no subitem **3.4.2. - Priorização dos Riscos para Tratamento**. Cada risco priorizado deve ser relacionado a uma opção de tratamento. A escolha da opção depende do nível do risco, conforme apresentado no Quadro 8, a seguir:

QUADRO 8: OPÇÕES DE TRATAMENTO DO RISCO	
OPÇÃO TRATAMENTO	DESCRIÇÃO
MITIGAR	Um risco normalmente é mitigado quando é classificado como “Alto” ou “Extremo”. A implementação de controles, neste caso, apresenta um custo/benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
COMPARTILHAR	Um risco normalmente é compartilhado quando é classificado como “Alto” ou “Extremo”, mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro.
EVITAR	Um risco normalmente é evitado quando é classificado como “Alto” ou “Extremo” e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco. Evitar o risco pode significar encerrar um processo organizacional. Nesse caso, essa opção deve ser aprovada pela área de atuação estratégica.
ACEITAR	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Se a opção de tratamento do risco for MITIGAR, devem ser definidas medidas de tratamento e controle para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível das faixas de apetite a risco (risco “Baixo” ou “Médio”), conforme o **Quadro 7 – Atitude perante o risco para cada classificação**, tratado acima na etapa de Priorização dos Riscos para Tratamento (**subitem 3.4.2.**). O Apetite a Risco ou Grau de Tolerância a Riscos dos principais *stakeholders* da empresa pode ser revisto sempre que necessário.

As informações produzidas nesta etapa, referentes às opções de tratamento dos riscos e propostas de projetos/ações para tratamento e controle dos riscos, deverão ser registradas como “respostas aos riscos”, no **Anexo 7.2 (Formulário 5 – Registro das Informações para Gerenciamento dos Riscos)**, disponível ao final deste documento.

3.4.4. Definição de Medidas de Tratamento e Controle e Elaboração do Plano de Tratamento

A área de atuação operacional, com auxílio da área de atuação tática, elaborará um plano de ação – Plano de Tratamento – para a implementação das medidas de tratamento e controle dos riscos nos processos organizacionais. Esse plano de tratamento deve conter, pelo menos:

- Evento de risco que se deseja tratar;
- Projeto ou ação que implementará um conjunto de medidas de tratamento e controle;
- Medida(s) de tratamento e controle contemplada(s) no projeto ou ação incluindo reserva de contingência, dentre outras medidas;
- Objetivos/benefícios esperados com a implementação da(s) medida(s) de tratamento e controle;
- Área organizacional responsável pela implementação da(s) medida(s) de tratamento e controle;
- Áreas organizacionais corresponsáveis pela implementação da(s) medida(s) de tratamento e controle, isto é, áreas envolvidas na implementação dessa(s) medida(s);
- Servidor responsável pela implementação das medidas de tratamento e controle, que também deverá monitorar e reportar sua evolução;
- Breve descrição sobre a implementação: como será implementada a medida de tratamento e controle;
- Custo estimado para a implementação, prevendo reserva de contingência;
- Data prevista para início da implementação;
- Data prevista para o término da implementação;
- Situação/acompanhamento da implementação das medidas de tratamento e controle contempladas no projeto ou ação.

Se as iniciativas definidas no Plano de Tratamento envolverem mais de uma área, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de plano para que essas áreas validem as iniciativas de que participarem. Após sua elaboração, o Plano de Tratamento deve ser aprovado pela área de atuação estratégica.

Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

Para proposição de novos controles é importante que, em uma primeira abordagem da elaboração do Plano de Tratamento, avalie-se a necessidade de melhorar ou extinguir controles já existentes. As informações pertinentes deverão ser preenchidas no formulário oferecido no **Anexo 7.2 (Formulário 6 – Plano de Tratamento dos Eventos de Risco)**, disponível ao final deste documento.

3.4.5. Validação do Resultado do Processo de Gerenciamento de Riscos

O resultado do processo de gerenciamento de riscos (entendimento do contexto, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos e definição de respostas aos riscos) de cada processo organizacional selecionado deve ser avaliado e validado pela área de atuação estratégica da empresa.

Após a validação do resultado, a área de atuação estratégica deverá:

- Encaminhar esse resultado às áreas da empresa para conhecimento;
- Incluir as iniciativas previstas no Plano de Tratamento, nas metas e atividades das respectivas áreas;
- Encaminhar o Plano de Tratamento aprovado às áreas corresponsáveis pelas iniciativas para que estas também incluam as ações em suas metas e atividades.

3.4.6. Implementação do Plano de Tratamento

A implementação do Plano de Tratamento envolve a participação da área responsável pelo processo organizacional e das áreas corresponsáveis, caso existam outras áreas envolvidas na implementação das medidas de tratamento e controle.

A responsabilidade primária pelo Plano de Tratamento permanece com a área responsável por cada processo organizacional analisado. No Plano de Tratamento, deve ser indicado o servidor responsável pela implementação das medidas de tratamento e controle, que também deverá monitorar e reportar a evolução destas medidas.

3.5. Monitoramento e análise crítica

Monitoramento e análise crítica envolve verificação e supervisão crítica contínua, visando identificar mudanças no desempenho requerido ou esperado para determinar a adequação, suficiência e eficácia da gestão de riscos.

O monitoramento no âmbito do processo de gerenciamento de riscos deve ser realizado pela área de atuação operacional responsável pelo processo organizacional, em conjunto com a área de atuação tática, de forma a:

- Garantir que os controles sejam eficazes e eficientes;
- Analisar as ocorrências dos riscos;
- Detectar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento;
- Identificar os riscos emergentes. O Decreto Estadual (nº 33.805, 09 novembro de 2020), também delega a todos colaboradores da empresa, a responsabilidade de comunicar a situação dos níveis de riscos e da efetividade das medidas de controle implementadas.

3.6. Registro e relato

Esta etapa contempla as atividades referentes ao registro documental e relato das atividades por meio de mecanismos apropriados para fornecer informações para tomada de decisão.

É importante documentar e relatar cada etapa do processo de gerenciamento de riscos.

As etapas de Registro e o Relato visam:

- Comunicar as atividades e os resultados do gerenciamento de riscos em toda a organização;
- Fornecer informações para tomada de decisão;
- Aperfeiçoar o processo de gerenciamento de riscos;
- Auxiliar a interação entre as partes interessadas.

A área responsável pelo processo organizacional disponibilizará as informações adequadas quanto ao gerenciamento de riscos dos processos sob sua responsabilidade a todos os níveis da empresa e demais partes interessadas. Cabe à instância de atuação tática requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais.

3.6.1. Registro

É importante que as decisões relativas à criação, retenção e manuseio de informações documentadas levem em consideração o seu uso, a sensibilidade da informação e os contextos interno e externo.

Frequentemente, a documentação do processo de gerenciamento de riscos é exigida para demonstrar conformidade com requisitos legais ou para mostrar a devida diligência, devendo ser composta, preferencialmente, por:

- A descrição do contexto interno e externo;
- Papéis, responsabilidades e responsabilizações pelo gerenciamento de riscos na organização;
- O plano de comunicação e consulta;
- Procedimento sobre o processo de gerenciamento de riscos, incluindo os critérios de risco da organização, planos de tratamento de riscos, entre outras informações documentadas nas diversas etapas do processo.

3.6.2. Relato

O Relato é parte integrante da governança da empresa. Tem como objetivo melhorar a qualidade da comunicação entre as partes interessadas e auxiliar a direção superior na tomada de decisões. Diversos fatores devem ser considerados para que o relato alcance seu objetivo. dentre eles:

- Identificação das partes interessadas e suas necessidades específicas de informação;
- Custo, frequência e pontualidade do relato;
- Método de relato;
- Pertinência da informação para o alcance dos objetivos organizacionais e para a tomada de decisão.

É importante a identificação das necessidades pelas partes interessadas para que sejam definidos relatórios padronizados para apresentação dos resultados para os *stakeholders*.

4. CONSIDERAÇÃO FINAL

A elaboração do PGR da Etice é um marco na história da empresa e a coloca em sintonia com as boas práticas internacionais de gestão. Ressalte-se que a adequada implementação do mesmo requer um alto investimento da alta administração na comunicação, treinamento dos colaboradores pois o engajamento dos mesmos é essencial no planejamento, bem como na execução das ações de mitigação.

Como recomendação, sugere-se para os próximos passos a implementação de um projeto piloto, no qual será testada e adequada a metodologia de gerenciamento de riscos apresentada, bem como elaborados guias sumarizados para direcionar as execuções do Plano de Gerenciamento de Riscos (PGR) em cada área de atuação da empresa.

5. REFERÊNCIAS

- **Lei Federal nº 13.303/2016** – DISPOSIÇÕES APLICÁVEIS ÀS EMPRESAS PÚBLICAS E ÀS SOCIEDADES DE ECONOMIA MISTA (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm);
- **Decreto Estadual nº 33.805/2020** – POLÍTICA DE GESTÃO DE RISCOS DO PODER EXECUTIVO DO ESTADO DO CEARÁ (<https://www.cge.ce.gov.br/wp-content/uploads/sites/20/2020/11/Decreto-33805-2020-Politica-de-Gestao-de-Riscos-do20201110p01.pdf>);
- **Portaria nº 05/2021 da CGE** – METODOLOGIA DE GERENCIAMENTO DE RISCOS DO PODER EXECUTIVO DO ESTADO DO CEARÁ (https://www.cge.ce.gov.br/wp-content/uploads/sites/20/2021/02/do20210209p01-PORTARIA-No05_2021..pdf);
- Norma ABNT ISO 31.000/2009 – GESTÃO DE RISCOS (<http://www.abnt.org.br/imprensa/releases/5828-abnt-publica-a-versao-abnt-nbr-iso-31000-gestao-de-riscos>);
- **Lei Estadual nº 16.717/2018** – PROGRAMA DE INTEGRIDADE DO PODER EXECUTIVO DO ESTADO DO CEARÁ (<https://belt.al.ce.gov.br/index.php/legislacao-do-ceara/organizacao-tematica/trabalho-administracao-e-servico-publico/item/6534-lei-n-16-717-de-21-12-18-d-o-26-12-18>);
- **Decreto Estadual nº 32.792/2018** – DISTRIBUIÇÃO E DENOMINAÇÃO DOS CARGOS DE PROVIMENTO EM COMISSÃO DA EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ - ETICE (<https://www.etice.ce.gov.br/wp-content/uploads/sites/5/2018/08/Novo-Estatuto-da-Etice.pdf>).

6. GLOSSÁRIO

O glossário é um elemento pós-textual que visa apresentar a lista de determinados termos técnicos e conceitos que foram utilizados neste documento sobre gerenciamento de riscos para facilitar a compreensão dos leitores.

Os seguintes termos e definições listados têm como base o Art. 3º do Decreto nº 33.805 de 09/11/2020 DOE 10/11/2020 que instituiu a Política de Gestão de Riscos (PGR) do Poder Executivo do Estado do Ceará e a Norma ABNT NBR ISO 31000:2009:

- Plano de gestão de riscos (aplicável a um determinado produto, processo e projeto, em parte ou em toda a organização): esquema dentro da **estrutura da gestão de riscos**, que especifica a abordagem, os componentes de gestão (procedimentos, práticas, atribuição de responsabilidades, sequência e cronologia das atividades) e os recursos a serem aplicados para gerenciar riscos. (ABNT)
- Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar um produto, resultado ou serviço predefinido. (PGR)
- Governança: combinação de processos e estruturas implantadas pela alta gestão da organização, para informar, dirigir, administrar, avaliar e monitorar suas atividades organizacionais, com o intuito de alcançar seus objetivos e prestar contas dessas atividades à sociedade. (PGR)
- Objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização. (PGR)
- Meta: quantificação do objetivo a ser alcançado. (PGR)
- Risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização. (PGR)
- Risco inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que reduzam ou possam reduzir a probabilidade de sua ocorrência ou de seu impacto. (PGR)
- Risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco. (PGR)
- Gestão de riscos: conjunto de ações coordenadas e direcionadas ao desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, de projetos e da eficácia na alocação e utilização dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da organização. (PGR)
- Gerenciamento de risco: processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar os objetivos, processos de trabalho e projetos da organização. (PGR)
- 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, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados. (PGR)

- Análise crítica (pode ser aplicada à estrutura da gestão de riscos, ao processo de gestão de riscos, ao risco ou ao controle): atividade realizada para determinar a adequação, suficiência e eficácia do assunto em questão para atingir os objetivos estabelecidos. (ABNT)
- Estrutura da gestão de riscos: conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua do gerenciamento de riscos de toda a organização. (ABNT)
- Política de gestão de riscos: declaração das intenções e diretrizes gerais de uma organização, relacionadas ao gerenciamento dos riscos a organização/instituição. (ABNT)
- Processo de gerenciamento de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos. (ABNT)
- Atitude perante os riscos: abordagem da organização para avaliar e eventualmente buscar, reter, assumir ou afastar-se dos riscos. (ABNT)
- Apetite a risco: nível de risco que uma organização está disposta a aceitar. (PGR)
- Proprietário do risco: pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco. (ABNT)
- Estabelecimento do contexto: definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos. (ABNT)
- Contexto externo (pode incluir o ambiente cultural, social político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, regional ou local, bem como os fatores-chaves e as tendências que tenham impacto sobre os objetivos da organização, e as relações com partes interessadas externas e suas percepções e valores): ambiente externo no qual a organização busca atingir seus objetivos. (ABNT)
- Contexto interno (pode incluir governança, estrutura organizacional, funções e responsabilidades; políticas, objetivos e estratégias implementadas para atingi-los; capacidades compreendidas em termos de recursos e conhecimentos (por exemplo: capital, tempo, pessoas, processos, sistemas e tecnologias); sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais quanto informais); relações com partes interessadas internas, e suas percepções e valores; cultura da organização; normas, diretrizes e modelos adotados pela organização; e forma e extensão das relações contratuais): ambiente interno no qual a organização busca atingir seus objetivos. (ABNT)

- Processo de avaliação de riscos: processo global de identificação de riscos, análise de riscos e avaliação de riscos. (ABNT)
- Identificação de riscos (envolve a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais e pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas e as necessidades das partes interessadas): processo de busca, reconhecimento e descrição de riscos. (ABNT)
- Fonte de riscos (pode ser tangível ou intangível): elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco. (ABNT)
- Perfil de risco: descrição de um conjunto qualquer de riscos. O conjunto de riscos pode conter riscos que dizem respeito a toda a organização, parte da organização, ou referente ao qual tiver sido definido. (ABNT)
- Evento (pode consistir em uma ou mais ocorrências e pode ter várias causas; em alguma coisa que não ocorrer; algumas vezes ser referido como um “incidente” ou um “acidente”; um evento sem consequências pode ser referido como um “quase acidente” ou um “incidente” ou “por um triz”): ocorrência ou mudança em um conjunto específico de circunstâncias. (ABNT)
- Consequência: resultado de um evento que afeta positiva ou negativamente os objetivos. Um evento pode levar a uma série de consequências. Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos sobre os objetivos. As consequências podem ser expressas qualitativa ou quantitativamente. As consequências iniciais podem desencadear reações em cadeia. (ABNT)
- Análise de riscos: processo de compreender a natureza dos riscos e determinar o nível dos riscos analisados. A análise de riscos fornece a base para a avaliação de riscos, para as decisões sobre o tratamento de riscos e inclui a estimativa de riscos. (ABNT)
- Nível de risco: criticidade do risco, assim compreendida a intensidade do impacto de um risco nos objetivos, processos de trabalho e Organização, a partir de uma matriz pré-definida. (PGR)
- Impacto: efeito resultante da ocorrência do evento.
- Probabilidade: chance de um evento algo ocorrer. (ABNT)
- Tratamento de riscos: processo para moderar/minimizar/modificar o risco. O tratamento de risco pode envolver: a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; assumir ou aumentar o risco, a fim de buscar uma oportunidade; a remoção da fonte de risco; a alteração da probabilidade; a alteração das consequências; o compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco); e a retenção do risco por uma escolha consciente. Os tratamentos de riscos relativos às consequências negativas são muitas vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos" e "redução de riscos". O tratamento de riscos pode criar novos riscos ou modificar riscos existentes. (ABNT)
- Reserva de contingência: consiste em uma reserva orçamentária para o cronograma de atividades a ser utilizada para remediar o impacto dos resíduos dos riscos que ocorrerem ou seja só será executada quando o risco ocorrer

- Plano de contingência: é um documento desenvolvido com o intuito de desenvolver, avaliar, uniformizar, organizar, orientar as ações necessárias para as respostas de controle e combate às ocorrências anormais e adversas.
- Controle: medida que pode modificar o **risco**. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco. Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido. (ABNT)
- Medida de controle: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados. (PGR)
- Monitoramento: verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. O monitoramento pode ser aplicado à estrutura da gestão de riscos, ao processo de gestão de riscos, ao risco ou ao controle. (ABNT)

7. ANEXOS

7.1. MATRIZ DE RESPONSABILIDADES (RACI)

MATRIZ RACI						
ATIVIDADES	ÁREA DE ATUAÇÃO ESTRATÉGICA	ÁREA DE ATUAÇÃO TÁTICA	ÁREA DE ATUAÇÃO OPERACIONAL	GESTOR DA ÁREA	RESPONSÁVEL POR GERENCIAMENTO DE RISCOS	COLABORADORES
Selecionar processos críticos	A	I	C	R	C	I
Identificar os responsáveis pelos processos selecionados	I	I	C	R	C	I
Definir níveis de apetite a riscos dos processos selecionados	A	C	R	C	C	I
Realizar entendimento do contexto da empresa	I	C	R	C	A	I
Realizar identificação dos riscos para processos críticos	I	C	R	C	A	I
Realizar a análise dos riscos	I	C	R	C	A	I
Realizar a avaliação dos riscos – calcular risco inerente, classificar o risco, calcular risco residual	I	C	R	C	A	I
Realizar a avaliação dos riscos – avaliar eficácia dos controles internos existentes em relação aos objetivos do processo	R	I	C	C	A	I
Realizar a identificação dos riscos que serão priorizados para tratamento	A	C	R	C	C	I
Definir respostas aos riscos	A	C	R	C	C	I
Elaborar Plano de Contingência (PC – medidas de tratamento e controle)	A	C	R	C	C	I
Implementar o PC	I	I	R	C	C	I
Realizar monitoramento	I	R	R	R	R	I
Realizar análise crítica dos níveis de riscos e da efetividade do PC	I	R	C	C	C	I
Avaliar desempenho do gerenciamento de riscos e fortalecer a aderência dos processos à conformidade normativa	R	C	C	C	C	I
Documentar e relatar cada etapa do gerenciamento de riscos – Registro e Relato	I	R	C	C	C	I

Responsável (R): executa a atividade; **Autoridade (A):** aprova a tarefa ou produto/pode delegar a função, mas mantém a responsabilidade; **Consultado (C):** pode agregar valor ou é essencial para a implementação do plano; **Informado (I):** deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver diretamente nas decisões.

7.2. FORMULÁRIOS CONSOLIDADOS

FORMULÁRIO 1: PLANO DE COMUNICAÇÃO E CONSULTA				
Data	Descrição	Responsável	Público Alvo/ Participantes	Status
	Divulgação geral da implantação do processo de gerenciamento de riscos			
	Definição dos processos críticos da empresa (2 por área de atuação)			
	Identificação e avaliação de riscos (matriz de riscos por processo)			

Nota: **Data:** dia, mês e ano em que o evento deverá ocorrer; **Descrição:** detalhamento do evento; **Responsável:** pessoa que conduzirá o evento; **Público Alvo/Participantes:** pessoas/público que o evento deve atingir; **Status:** evento “Previsto”, “Em execução” e “Finalizado”.

FORMULÁRIO 2: IDENTIFICAÇÃO E ANÁLISE DE RISCOS							
Processo/Etapa (1)	Objetivo (2)	Evento de Risco (3)	Categoria (4)	Causa (5)	Consequência (6)	Controles	
						Preventivo (7)	Atenuação e recuperação (8)

Nota: Estas informações, também deverão compor, posteriormente, o **Formulário 5 – Registro das Informações para Gerenciamento dos Riscos**, disponível mais adiante.

FORMULÁRIO 3: AVALIAÇÃO DOS RISCOS				
Probabilidade (9)	Impacto (10)	Risco Inerente (11)	Avaliação dos Controles (12)	Risco Residual (13)

Nota: As colunas de 9 a 13 deverão compor também o **Formulário 6 – Opções de Tratamento dos Riscos**.

FORMULÁRIO 4: PRIORIZAÇÃO DOS RISCOS		
Classificação (14)	Priorizado (15)	Justificativa (16)

Nota: As colunas de 14 a 16 deverão compor também o **Formulário 5 – Registro das Informações para Gerenciamento dos Riscos**.

