POLÍTICAS DE CONFORMIDADE E GERENCIAMENTO DE RISCOS

CEASA/ES

Novembro 2024

Av. Mário Gurgel, 5468 – Vila Capixaba, Cariacica – ES, CEP – 29148-906
Tel. (27) 3336-1603 • ceasa@ceasa.es.gov.br • www.ceasa.es.gov.br

RESOLUÇÃO 001/2024

Dispõe sobre a Política de Conformidade e Gestão de Riscos da Centrais de Abastecimento do Espírito Santo S/A - Ceasa/ES e dá outras providências.

A Diretoria Executiva da CENTRAIS DE ABASTECIMENTO DO ESPÍRITO SANTO S/A – CEASA/ES, no uso das atribuições estatutárias, e;

Considerando o contido na Lei Federal nº 13.303/2016, em seu art. 9º, que estabelece a necessidade de criação de um Código de Conduta e Integridade, bem como de normas de Gerenciamento de Riscos e Controle Interno, que devem reger as empresas públicas e as sociedades de economia mista;

Considerando o Decreto Estadual nº 4272-R de 26 de junho de 2018, que dispõe sobre as regras de governança e tratamento diferenciado para empresas estatais de menor porte;

Considerando os valores da Ceasa-ES, principalmente no que tange a Ética, Segurança, Transparência e a Eficiência;

Considerando o que compete à Assessoria de Conformidade e Gerenciamento de Riscos, previsto no Estatuto Social no art. 35, §2º, inciso I, de propor a Política de Conformidade de Gerenciamento de Riscos para a sociedade;

Considerando que a Diretoria da Ceasa-ES possui competência para dispor sobre a organização administrativa da organização, bem como monitorar a sustentabilidade dos negócios, os riscos estratégicos e as respectivas medidas de mitigação dos mesmos, nos termos do inciso III e VI do art. 13 do Estatuto Social;

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1º - Instituir a POLÍTICA DE CONFORMIDADE E GERENCIAMENTO DE RISCOS DA CEASA-ES.

§ 1º - Esta Política de Conformidade e Gestão de Riscos é parte integrante do sistema de governança e gestão, que suporta a concepção, implementação e melhoria contínua na estrutura organizacional da Centrais de Abastecimento do Espírito Santo S/A – CEASA/ESES.

§ 2º - Esta norma se aplica a todos os Administradores, gerentes, membros de comissões, servidores, comissionados, contratados, permissionários, produtores, atacadistas, fornecedores em geral, bem como a todos aqueles que, direta ou indiretamente, se relacionem com a Ceasa-ES, aos quais cabe alertar a área de Gestão de Riscos e, por consequência, a Diretoria Executiva, sobre os riscos envolvidos na execução dos procedimentos sob sua responsabilidade.

Art. 2º - A Política de Gestão de Riscos tem como premissa o alinhamento ao Planejamento Estratégico do Governo do estado do Espírito Santo, bem como, aos objetivos estratégicos da Ceasa-ES, definidos em seu Plano Estratégico.

Art. 3º - São elementos estruturantes da Gestão de Riscos da Ceasa-ES, o Estatuto Social, a Política de Conformidade e Gestão de Riscos, o Código de conduta e Integridade e a Assessoria Especial de Conformidade e Gerenciamento de Riscos.

CAPÍTULO II

DOS CONCEITOS

Art. 4º - Para melhor entendimento e compreensão desta Norma entende-se como:

- ✓ **Administradores:** Os Membros do Conselho de Administração e da Diretoria Executiva.
- ✓ **Análise de riscos:** Processo para compreender a natureza do risco e determinar o nívelde risco. Fornece a base para a avaliação dos riscos, bem como para as decisões quanto ao tratamento dos riscos;
- ✓ **Gestão de riscos:** Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a Instituição, destinado a fornecer segurança razoável quanto à realização de seus objetivos;
- ✓ **Área de Gestão de Riscos:** Área responsável por atividades coordenadas para dirigir e controlar os riscos, envolvendo atividades de implantação da metodologia, de identificação, análise, avaliação, priorização, resposta ao risco, tratamento, comunicação/consulta, monitoramento e revisão de riscos;
- ✓ **Gerenciamento de riscos:** É a aplicação do sistema implantado na Instituição, de modo a identificar, em todos os níveis e unidades, quais são

os eventos capazes de impactar seus objetivos, visando adotar medidas de tratamento de riscos, mantendo-os em conformidade com o nível definido como tolerável;

- ✓ **Governança:** combinação de processos e estruturas implantadas pela alta administração da empresa, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;
- ✓ **Controle interno:** Conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável para a consecução da missão da Instituição;
- ✓ **Estrutura da gestão de riscos:** Conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implantação, monitoramento, análise crítica e melhoria contínua da gestão de riscos;
- ✓ **Avaliação de riscos**: Processo para estimar o potencial dos riscos, e decidir se o risco é ou não tolerável, bem como propor formas de mitigação dos riscos constatados;
- ✓ **Comunicação e consulta:** Processos contínuos e iterativos que uma Instituição conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos;
- ✓ **Conformidade (*Compliance*):** Pilar da Governança Corporativa que fortalece o Sistema de Controles Internos e dissemina a cultura de cumprimento das normas aplicáveis, as políticas internas, o Código de Conduta e Integridade, agindo com ética e integridade;
- ✓ **Critérios de riscos:** Termos de referência contra os quais o significado de um risco é avaliado;
- ✓ **Evento:** Ocorrência ou alteração em um conjunto específico de circunstâncias no contexto interno e/ou externo;
- ✓ **Fator de risco:** Elemento que, individualmente ou combinado, possui potencial intrínseco para dar origem ao risco;
- ✓ **Identificação de riscos:** Processos de busca, reconhecimento e descrição de riscos;
- ✓ **Incerteza:** Deficiência de informações de um evento, sua compreensão, seu conhecimento, sua probabilidade, sua consequência ou impacto;
- ✓ **Impacto:** Efeito resultante da ocorrência do evento;
- ✓ **Medida de Controle:** Medida aplicada para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais sejam alcançados;

- ✓ **Meta:** Alvo ou propósito com que se define um objetivo a ser alcançado;
- ✓ **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;
- ✓ **Nível de risco:** Magnitude de um risco, expressa em termos da combinação das probabilidades e dos impactos dos riscos;
- ✓ **Objetivo Organizacional:** Situação que se deseja alcançar de forma a evidenciar o êxito no cumprimento da missão e no atingimento de sua visão de futuro;
- ✓ **Processo:** É um conjunto de atividades com uma ordenação específica, com uma ou mais entradas, que cria saída de valor para o cliente e possui começo e fim claramente identificados, podendo subdividir-se em sub processos;
- ✓ **Risco:** Possibilidade de ocorrência de um evento ou condição incerta, que possa ter impacto, positivo ou negativo, no cumprimento dos objetivos de um processo;
- ✓ **Risco Estratégico:** É o risco associados à tomada de decisão da alta administração, que podem gerar perda substancial no valor econômico da Instituição;
- ✓ **Risco inerente:** É o risco a que uma Instituição está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou impacto;
- ✓ **Risco residual:** é o risco a que uma Instituição está exposta após a implementação de ações gerenciais para o tratamento do risco;
- ✓ **Tratamento de riscos:** Processo para modificar os riscos da Política de Gestão de Riscos corporativos.

CAPÍTULO III

DO OBJETIVO

Art. 5º - A Política de Gestão de Riscos tem por objetivo estabelecer os princípios, as diretrizes, as responsabilidades e o processo de gestão de riscos na Centrais de Abastecimento do Espírito Santo S/A — Ceasa-ES, com vistas à incorporação da análise de riscos à tomada de decisão, em conformidade com as boas práticas de governança adotadas no setor público.

§ 1º - O principal objetivo da Gestão de Riscos é criar uma estrutura de suporte para identificar, medir, monitorar e gerenciar os diversos tipos de riscos, os quais a Ceasa-ES está exposta, contribuindo para alcançar as metas estabelecidas no planejamento estratégico e na gestão operacional.

§ 2º - A Política definida nesta Portaria deverá ser observada por todas as áreas e níveis de atuação da Ceasa-ES, sendo aplicáveis a seus respectivos processos de trabalho, projetos, atividades e ações.

CAPÍTULO IV

DOS COMPROMISSOS DA POLÍTICA DE GESTÃO DE RISCOS

Art. 6º - A Política de Gestão de Riscos da Ceasa-ES tem por compromisso o desenvolvimento, disseminação e implantação de uma metodologia de gerenciamento de riscos institucional, objetivando apoiar a melhoria contínua da implantação de metodologia de gestão de riscos, por meio da identificação dos riscos e a alocação e utilização eficaz dos recursos disponíveis. Dentre outros compromissos, temos ainda:

I. Aumentar a probabilidade de alcance dos objetivos estratégicos da Ceasa-ES;
II. Proporcionar um ambiente saudável e seguro às pessoas, ao patrimônio e às operações;
III. Fomentar uma gestão proativa, com Eficácia e Eficiência nos processos organizacionais;
IV. Atentar para a necessidade de se identificar e tratar riscos em toda a Ceasa-ES;
V. Facilitar a identificação de oportunidades e ameaças;
VI. Prezar pelas conformidades legais e normativas dos processos organizacionais;
VII. Melhorar a prestação de contas aos Órgãos de Controle – Interno e Externo;
VIII. Aprimorar a governança corporativa, por meio do fortalecimento das áreas estatutárias;
IX. Estabelecer uma base confiável para a tomada de decisão;
X. Promover a melhoria contínua do desempenho e do controle interno da gestão;
XI. Garantir a proteção dos ativos, tangíveis e intangíveis;
XII. Garantir a confidencialidade, integridade e disponibilidade das informações;
XIII. Melhorar a prevenção de perdas e a gestão de incidentes;
XIV. Melhorar a aprendizagem organizacional, disseminando a cultura da importância dos controles internos a todos os empregados e prestadores de serviço; e
XV. Aumentar a capacidade da empresa de se adaptar a mudanças;

Art. 7º - A Política de Gestão de Riscos promoverá:

I. A identificação de eventos em potencial que possam afetar a consecução dos objetivos institucionais da Ceasa-ES;
II. O alinhamento do apetite ao risco com as estratégias adotadas;
III. O fortalecimento das decisões em resposta aos riscos;
IV. O aprimoramento dos controles internos administrativos.

Art. 8º - A Política de Gestão de Riscos Corporativos da Ceasa-ES estabelece diretrizes para o gerenciamento de riscos e define a metodologia utilizada, a fim de contribuir com os gestores para o tratamento das incertezas identificadas com eficácia, visando a mitigação dos riscos existentes.

§ 1º - O reconhecimento dos riscos requer que a administração analise as informações em relação aos ambientes interno e externo, e utilize seus recursos, bem como ajuste as atividades frente aos riscos levantados, visando a melhoria dos controles internos.

§ 2º - A Gestão de Riscos deve estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional da Ceasa-ES.

CAPÍTULO V

DOS PRINCÍPIOS

Art. 9º - A Política de Conformidade e Gestão de Riscos é parte integrante de todas as atividades organizacionais, e deve seguir os seguintes Princípios, que servem de critérios para avaliar sua eficácia e eficiência depois de instaurados:

I. Agregar valor e proteger o ambiente interno da Ceasa-ES;
II. Ser parte integrante de todos os processos organizacionais;
III. Subsidiar a tomada de decisões dos gestores e da alta administração;
IV. Abordar explicitamente as incertezas;
V. Ser sistemática, estruturada, oportuna e abrangente;
VI. Ter base nas melhores práticas e informações disponíveis;
VII. Considerar fatores humanos e culturais;
VIII. Ser personalizada, transparente e inclusiva;
IX. Ser dinâmica, iterativa e capaz de reagir a mudanças;
X. Apoiar a melhoria contínua da Ceasa-ES.

CAPÍTULO VI

DAS TIPOLOGIAS

Art. 10 - A Política de Gestão de Riscos Corporativos da Ceasa-ES deverá abranger as seguintes tipologias de risco ao efetuar seu mapeamento e avaliação, considerando os contextos Interno e Externo:

I. **Conformidade:** Riscos decorrentes do órgão/entidade não ser capaz ou hábil para cumprir com as legislações aplicáveis ao seu negócio e não elabore, divulgue e faça cumprir suas normas e procedimentos internos;

II. **Recursos Humanos:** Riscos decorrentes da falta de capacidade ou habilidade da instituição em gerir seus recursos humanos de forma alinhada aos objetivos estratégicos definidos.

III. **Imagem:** Riscos de exposição negativa nos meios de comunicação e/ou perda de confiança das partes interessadas.

IV. **Tecnologia da Informação:** Riscos decorrentes da indisponibilidade ou inoperância de equipamentos e sistemas informatizados que prejudiquem ou impossibilitem o funcionamento ou a continuidade normal das atividades da instituição.

V. **Ambiental:** Riscos associados à gestão inadequada de questões ambientais, causando efeitos como: contaminação de solo, água ou ar, decorrente da disposição inadequada de resíduos, ou levando a acidentes com vazamento de produtos tóxicos, entre outros.

VI. **Estratégica:** Estão associados à tomada de decisão da alta administração e podem gerar perda substancial no valor econômico da organização, e resultar em falhas relevantes nas demonstrações financeiras.

VII. **Financeira:** São aqueles associados à exposição das operações financeiras da Companhia.

VIII. **Integridade/Fraude:** Referem-se aos riscos de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possa comprometer os valores preconizados no Mapa Estratégico da Ceasa-ES.

IX. **Legal/Compliance:** Risco relacionado à falta de habilidade ou disciplina da organização para cumprir com a legislação e/ou regulamentação externa aplicáveis ao negócio e às normas e procedimentos internos.

X. **Legal/Regulatório:** Risco de suspensão de licenças de funcionamento, ou de não atendimento a Políticas Públicas e regulamentos.

XI. **Operacional:** Riscos associados à possibilidade de ocorrência de perdas

resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, assim como de eventos externos como catástrofes naturais, fraudes, greves e outros.

Parágrafo Único - Os riscos identificados relacionados ao Combate a Corrupção deverão ser agrupados a fim de se avaliar o Nível de Risco consolidado, com vistas a priorizar as ações de tratamento adequados dos mesmos.

CAPÍTULO VII

DA PROBALIDADE DE OCORRÊNCIA E DO NÍVEL DOS IMPACTOS

Art. 11 - Todo risco decorre em função da probabilidade de sua ocorrência, com o nível das consequências de seus resultados, sendo o método e o nível de detalhamento da análise, influenciados pelos objetivos definidos pela norma, pela natureza do risco e pela disponibilidade de informações e de recursos envolvidos no processo. Desse modo, define-se a probabilidade de ocorrência e o nível do impacto, com base na percepção dos responsáveis pelos riscos em seus respectivos processos.

§ 1º - Eventos são situações em potencial que ainda não ocorreram, mas que podem causar impacto na consecução dos objetivos da organização, podendo ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades.

§ 2º - Por meio da identificação de eventos, pode-se planejar o tratamento adequado para as oportunidades e para os riscos, que devem ser entendidos como parte de um contexto, e não de forma isolada.

§ 3º - Em análises qualitativas e quantitativas, considerando que o nível de risco é proporcional tanto à probabilidade como ao impacto, considerar-se-á o Risco como um produto dessas duas variáveis.

✓ PROBABILIDADE DE OCORRÊNCIA

Muito baixa	Improvável, em situações excepcionais, o evento poderá até ocorrer.
Baixa	Rara, de forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.
Média	Possível, de alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
Alta	Provável, de forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.

Muito Alta	Praticamente certa, de forma inequívoca, o evento ocorrerá, onde as circunstâncias indicam claramente essa possibilidade.

- ✓ **NÍVEL DO IMPACTO** (caso o evento ocorra)

Muito Baixo	Mínimo impacto nos objetivos.
Baixo	Pequeno impacto nos objetivos.
Médio	Moderado impacto nos objetivos, porém recuperável.
Alto	Significativo impacto nos objetivos, de difícil reversão.
Muito Alto	Catastrófico impacto nos objetivos, de forma irreversível.

CAPÍTULO VIII

DA RESPOSTA AOS RISCOS

Art. 12 - Quanto à resposta aos Riscos, serão consideradas duas tipologias de Risco:

I. **Risco Inerente -** É o risco que uma organização terá de enfrentar na falta de medidas adotadas para alterar a probabilidade ou o impacto do evento;
II. **Risco Residual** - É aquele que ainda permanece após a resposta da administração.

Art. 13 - Considerando as tipologias do artigo anterior, a avaliação de riscos deverá ser aplicada primeiramente aos Riscos Inerentes, sendo que para cada risco identificado, deverá ser prevista uma resposta, que pode ser de 4 tipos:

- ✓ Evitar;
- ✓ Aceitar;
- ✓ Compartilhar; ou,
- ✓ Reduzir.

Parágrafo Único - Cada uma dessas respostas será aplicada conforme o nível do risco:

EVITAR	**Risco Crítico** - Promover ações que evitem, eliminem ou atenuem rapidamente as causas e/ou efeitos.
REDUZIR	**Risco Alto** - Adotar ações para reduzir a probabilidade ou impacto dos riscos, ou ambos.
COMPARTILHAR	**Risco Moderado** - Reduzir a probabilidade ou impacto pela transferência ou mesmo compartilhamento de uma parte do risco, através de Seguros ou terceirização das atividades.
ACEITAR	**Risco Pequeno** - Conviver com o evento de risco, mantendo as práticas e procedimentos existentes.

CAPÍTULO IX

DAS ATIVIDADES DE CONTROLE

Art. 14 - A Administração da Ceasa-ES deve estabelecer e aplicar procedimentos de controle para auxiliar e assegurar que ações identificadas pelos responsáveis pelos processos, para tratar os riscos relacionados ao cumprimento dos objetivos da Organização, sejam realizadas de forma eficaz.

§ 1º - As atividades de controle deverão contribuir para que essas ações sejam eficazes e garantam que:

- ✓ Os objetivos sejam alcançados;
- ✓ As diretrizes administrativas sejam cumpridas;
- ✓ As regulamentações externas sejam atendidas;
- ✓ As ações necessárias para gerenciar os riscos estejam sendo implementadas.

§ 2º - As Atividades de Controle devem ser estabelecidas de forma tempestiva e adequadas, prevenindo e administrando os riscos inerentes ou em potencial da Ceasa-ES, devendo abranger os seguintes critérios:

- ✓ Atribuição de autoridade e limites de alçada;
- ✓ Revisão de superiores;
- ✓ Normatização Interna;
- ✓ Autorizações e Aprovações;
- ✓ Capacitação e Treinamento;
- ✓ Indicadores de Desempenho;
- ✓ Programas de Contingência e Planos de Continuidade dos Negócios.

§ 3º - A estrutura de controle interno deverá "reagir" de forma dinâmica, ajustando-se conforme as condições o determinem, em atividades continuas e independentes, ou uma combinação de ambas, para assegurar que os componentes de controle interno estejam presentes e funcionando.

CAPÍTULO X

DAS COMPETÊNCIAS E RESPONSABILIDADES PELA GESTÃO DE RISCOS

Art. 15 - São considerados Gestores de Riscos, em seus respectivos âmbitos e escopos de atuação, os Gestores ou Titulares dos processos de trabalho, projetos, atividades e ações desenvolvidos nos níveis estratégicos, táticos ou operacionais da Centrais de Abastecimento do Espírito Santo S/A — Ceasa-ES.

§ 1º - São considerados Agentes de Riscos, os colaboradores de cada setor, aos quais compete auxiliar os Gestores de Riscos no processo de avaliação e mensuração dos riscos, atuando como facilitadores, promovendo e acompanhando todas as fases desse processo, definidas nesta Norma.

§ 2º - A Administração da Ceasa-ES deve garantir a capacitação contínua de todos os colaboradores, principalmente dos Gestores e Agentes de Riscos, por meio de treinamento e atualizações dos processos de gestão.

Art. 16 - O principal componente do ambiente de controle é o comprometimento em todos os níveis da administração (Administradores e Gestores e Agentes de Riscos), com a qualidade do controle interno. Os fatores relacionados ao ambiente de controle incluem:

I. Integridade e valores éticos;
II. Competência das pessoas da entidade;
III. Estilo operacional da organização;
IV. Aspectos relacionados com a gestão;
V. Forma de atribuição da autoridade e responsabilidade.

Art. 17 - Compete ao CONAD:

I. Aprovar a Política de Gestão de Riscos da Ceasa-ES;
II. Atribuir formalmente a responsabilidade pela área de Gerenciamento de Riscos aos membros da Diretoria Executiva;
III. Garantir a Implementação e a supervisão das estruturas de gestão de riscos e de controle interno estabelecido para a prevenção e mitigação dos principais riscos estratégicos a que está exposta a Ceasa-ES.

Art. 18 - Compete aos Diretores:

I. Patrocinar a implantação da Política de Gerenciamento de Riscos;
II. Estabelecer a estratégia da Ceasa-ES, por meio do Planejamento Estratégico/Plano de Negócio e da estrutura de Gerenciamento de Riscos;
III. Criar e manter uma estrutura organizacional adequada para a supervisão e monitoramento dos controles dos riscos internos e externos;
IV. Supervisionar o desempenho dos controles internos da gestão;
V. Analisar e decidir sobre os riscos a serem assumidos pela Ceasa-ES;
VI. Garantir o cumprimento dos Planos de Ação das áreas sob sua responsabilidade, e o cumprimento das ações previstas, dentro dos prazos estabelecidos;

VII. Disponibilizar recursos necessários para o Processo de Gestão de Riscos;

VIII. Apoiar e incentivar o compromisso com o Processo de Gestão de Riscos, realizando treinamentos e reciclagens anuais, sobre esta política e suas atualizações.

Art. 19 - Compete à área de Gestão de Riscos:

I. Propor políticas de Conformidade e Gerenciamento de Riscos para a Sociedade, as quais deverão ser periodicamente revisadas e aprovadas pelo Conselho de Administração, e comunicá-las a todo o corpo funcional da organização;

II. Verificar a aderência da estrutura organizacional e dos processos, produtos e serviços da Sociedade às leis, normativos, políticas e diretrizes internas e demais regulamentos aplicáveis;

III. Comunicar à Diretoria Executiva, aos Conselhos de Administração e Fiscal a ocorrência de ato ou conduta em desacordo com as normas aplicáveis à Sociedade;

IV. Verificar a aplicação adequada do princípio da segregação de funções, de forma que seja evitada a ocorrência de conflitos de interesse e fraudes;

V. Verificar o cumprimento do Código de Conduta e Integridade, bem como promover treinamentos periódicos aos empregados e dirigentes da Sociedade sobre o tema;

VI. Coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a Sociedade;

VII. Coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados, verificando continuamente a adequação e a eficácia da gestão de riscos;

VIII. Estabelecer planos de contingência para os principais processos de trabalho da organização;

IX. Elaborar relatórios periódicos de suas atividades, submetendo-os à Diretoria Executiva, aos Conselhos de Administração e Fiscal;

X. Disseminar a importância da Conformidade e do Gerenciamento de Riscos, bem como a responsabilidade de cada área da Sociedade nestes aspectos; e,

XI. Outras atividades correlatas definidas pelo Diretor ao qual se vincula.

Art. 20 - Compete aos Gestores e/ou responsáveis pelos riscos, relativamente aos processos de trabalho e iniciativas sob sua responsabilidade, decidir sobre:

I. A escolha dos processos de trabalho que devam ter os riscos gerenciados e tratados em sua área, considerando a dimensão dos impactos que possam causar nos resultados de cada um de seus processos;

II. Definir os níveis de risco aceitáveis, considerando o previsto no Art. 14 desta Portaria;
III. Quais riscos deverão ser priorizados para tratamento por meio de ações de caráter imediato, a curto, médio ou longo prazos ou de melhoria contínua;
IV. As ações de tratamento e monitoramento dos riscos identificados, a serem implementadas, bem como, o prazo de implementação e o método de avaliação dos resultados obtidos com essas ações.

CAPÍTULO XI

DA COMUNICAÇÃO E INFORMAÇÃO

Art. 21 - A Administração deverá desenvolver um sistema de comunicação e informação, permitindo que todos os colaboradores da Ceasa-ES coletem e troquem informações necessárias para conduzir, gerenciar e controlar todas as suas operações relacionadas aos objetivos, riscos e controles.

§ 1º - A comunicação tem como propósito auxiliar todas as etapas do processo de Gestão de Riscos, de forma de permitir a comunicação eficiente. A eficácia dessa comunicação deverá ser ao longo de todo processo de Gestão de Riscos, tornando-se uma ferramenta de melhoria contínua.

§ 2º - O Plano de Comunicação deve ser estabelecido para assegurar que:
I. Todas as áreas compreendam claramente o papel, os objetivos, as funções e as responsabilidades da Área de Conformidade e Gerenciamento de Riscos, enquanto função de controle independente dentro da Ceasa-ES, bem como seus respectivos deveres e responsabilidades;
II. Todos os Servidores compreendam claramente os objetivos do processo de Gestão de Riscos, bem como os papéis, funções e as responsabilidades atribuídas aos diversos níveis hierárquicos da Ceasa-ES;
III. Todos os servidores tenham conhecimento dos meios de comunicação disponíveis para o processo de Gestão de Riscos, conforme o plano de comunicação definido;
IV. O programa de treinamento deverá abranger todos os funcionários da Ceasa-ES, observando seu grau de participação nas funções de Gestão de Riscos.

Art. 22 - A Ceasa-ES deve também desenvolver mecanismos para coletar informações do ambiente externo que possam afetá-la, e deve transmitir

externamente aquelas que sejam relevantes acs seus parceiros de negócio, inclusive à sociedade.

§ 1º - Essa comunicação deverá ser contínua e abordar aspectos financeiros, econômicos, operacionais e estratégicos, sendo um canal que movimente as informações em todas as direções, dos superiores aos subordinados e da Ceasa-ES para o ambiente externo, e vice-versa.

CAPÍTULO XII

DO PROCESSO DE GESTÃO DE RISCOS

Art. 23 - A operacionalização do processo de Gestão de Riscos da Ceasa-ES será compreendida pelas seguintes fases:

I. **Comunicação** - Processos contínuos e iterativos para compartilhar e obter informações de todas as equipes, com relação a gerenciar riscos;

II. **Estabelecimento do Contexto** - Definição dos parâmetros externos e internos, a serem considerados ao se estabelecer o escopo e os critérios de risco;

III. **Identificação dos Riscos** – Análise e descrição dos riscos, identificando as possíveis fontes e eventos de risco, bem como, suas causas e conseqüências potenciais;

IV. **Análise e Avaliação dos Riscos** - Processo de comparação e compreensão da natureza do risco e a mensuração do seu nível de criticidade, baseado nos critérios predeterminados no Art. 14 desta portaria;

V. **Tratamento dos Riscos** - Processo para modificar, resolver ou, pelo menos, mitigar o risco para que ele não seja mais uma ameaça para o processo em questão.

VI. **Monitoramento dos Riscos** - Monitoramento, supervisão, observação e identificação da situação de risco, executada de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado.

VII. **Identificação dos Controles** - Identificação dos procedimentos, ações ou documentos que garantam o alcance dos objetivos do processo e diminuam a exposição aos riscos.

VIII. **Estabelecimento dos Controles** - Políticas e procedimentos que assegurem o alcance dos objetivos da administração, diminuindo a exposição das atividades aos riscos, baseado no histórico de ocorrências, possibilitando antecipar possíveis novos riscos em todos os níveis e em todas as funções.

Parágrafo Único - Para a consecução da Identificação e da Análise dos Riscos dos processos e/ou procedimentos, poderão ser utilizadas soluções tecnológicas como instrumento de apoio à aplicação da metodologia da Gestão de Riscos a ser definida, desde que apresente os seguintes critérios:

I. Possibilidade de Interface com os demais sistemas de gestão da Ceasa-ES;
II. Classificação de Processos que sejam Críticos em uma Matriz de Riscos;
III. Elaboração de um Plano de Implementação de Controles;
IV. Visão integrada de Gestão de Riscos;
V. Inventário dos riscos, com a devida geração de relatórios, gráficos e estatísticas;
VI. Geração de indicadores de riscos, com o devido monitoramento contínuo e integrado;
VII. Gestão dos planos de Implementação de Controles.

Art. 24 - O processo de gestão de riscos deve ser objeto de revisão periódica, sempre que necessário ou em prazo não superior a 2 (dois) anos, abrangendo todos os processos de trabalho de todas as áreas de gestão da Ceasa-ES.

Parágrafo Único - O limite temporal a ser considerado para o ciclo de gestão de riscos de cada processo de trabalho será decidido pelo respectivo responsável pelo risco, levando em consideração o limite máximo estipulado no caput deste artigo.

Art. 25 - É dever de todos os responsáveis pelos processos internos e externos da Ceasa-ES, adequar constantemente suas práticas a esta Política e as demais regras de governança corporativa, na forma da lei e, proceder à difusão das regras contidas nesta norma, disseminando as boas práticas de integridade e governança nos ambientes em que se encontram e nas relações que se estabelecem.

Parágrafo Único - Inclui-se nesse dever, conhecer na íntegra o seu conteúdo, não podendo alegar desconhecimento, bem como, acompanhar todas as suas atualizações e interpretações, divulgadas anualmente pela Diretoria Executiva.

CAPÍTULO XIII

DAS DISPOSIÇÕES GERAIS

Art. 26 - A Ceasa-ES manterá registro formal de todos os atos administrativos provenientes do programa de Conformidade e Gerenciamento de Riscos, a fim de garantir o fornecimento de dados para as revisões periódicas internas, e para uso da controladoria e auditoria Interna e externa.

Parágrafo Único - Eventuais conflitos de atuação decorrentes do processo de gestão de riscos serão dirimidos pela Diretoria Executiva, com o apoio da área de Conformidade e Gerenciamento de Riscos.

Art. 27 - A Assessoria Especial de Conformidade e Gerenciamento de Riscos é a área responsável pela verificação do cumprimento dessas Políticas, sendo vinculada ao diretor presidente, conforme reza o estatuto social, bem como é a responsável por estabelecer os mecanismos necessários à sua implementação em todas as áreas da Ceasa-ES.

Art. 28 - Todas as ações relacionadas à Gestão de Riscos devem estar de acordo com o disposto nesta política, bem como dos normativos complementares, desenvolvidos para o detalhamento desta política.

Art. 29 - A Política de Conformidade e de Gestão de Riscos deverá ser implementada de forma gradual em todas as áreas da Ceasa-ES, com prioridade para os processos organizacionais que impactam diretamente no alcance de seus Objetivos Estratégicos.

Parágrafo Único - As exceções, eventuais violações e casos omissos à presente Política de Gestão de Riscos devem ser submetidas à apreciação da Diretoria Executiva.

Art. 30 - Todos os empregados, gestores e Diretores envolvidos na gestão de riscos devem manter sigilo absoluto sobre informações de acesso restrito, conforme ditames da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Art. 31 - A área de Conformidade e Gestão de Riscos, amparada pela respectiva Diretoria, é responsável pelas atualizações periódicas desta presente norma.

Art. 32 - A Diretoria Executiva da Ceasa-ES estabelecerá plano de comunicação entre as partes interessadas, internas e externas, para ampla divulgação destas Políticas.

Art. 33 - Esta Portaria entra em vigor na data de sua publicação.

Cariacica-ES, 11 de Novembro de 2024.

ANTÔNIO CARLOS CESQUIM DINIZ
DIRETOR PRESIDENTE
CEASA/ES

Antonio Carlos Cesquim Diniz
Diretor Presidente