INSTRUÇÃO NORMATIVA

N.º 004/2019

POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS DO SESI/RR

O Diretor Regional do SESI/RR, no uso de suas atribuições legais e regulamentares;

Considerando a necessidade de estabelecer no âmbito da instituição princípios, diretrizes e responsabilidades a serem observados no processo de Gerenciamento de Riscos Corporativos (GRC), de forma a possibilitar a adequada identificação, análise, avaliação, tratamento, monitoramento, análise crítica, melhoria contínua, comunicação e consulta;

RESOLVE:

Instituir a Política de Gestão de Riscos Corporativos do SESI/RR.

Art. 1º Para fins desta Instrução Normativa, considera-se:

- **Risco:** Efeito da incerteza nos objetivos presentes no Posicionamento Estratégico do Regional;
- **Riscos Corporativos:** Abrange os principais eventos de riscos estratégicos e operacionais, com a conexão direta nos Planos de Ação, traçados no Posicionamento Estratégico da instituição SESI/DR-RR, que impactam nas atividades previstas;
- **Riscos Estratégicos:** Representa a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e ambiente tecnológico, ou de eventos externos. Podem acarretar a interrupção ou morosidade das atividades dentro dos núcleos da entidade, bem como falhas em sistemas e infraestruturas de tecnologia da informação. Devem estar relacionados diretamente ao Posicionamento Estratégico da entidade, em voga;
- **Atitude Perante ao Risco:** É o nível de risco que a entidade se sujeita a aceitar na busca e na realização de sua estratégia;
- **Nível de Risco:** Relacionamento entre as probabilidades e consequências de um risco ocorrer;
- **Cultura de Riscos:** A cultura de risco são os valores, princípios, conhecimento e compreensão sobre risco que é compartilhado por um grupo de pessoas que têm um

propósito comum. Por meio dela, são identificados os elementos culturais adversos ou conflitantes e formas para tentar resolvê-los;

- **Inteligência de Riscos:** Capacidade para lidar com incertezas de forma lógica e racional; Aceitação das próprias limitações de conhecimento sobre a organização; Curiosidade e disposição para testar hipóteses diversas e antagônicas na organização; Habilidade para estimar probabilidades e consequências e saber como comunicar os tratamentos propostos;

- **Proprietário de Risco:** O proprietário responsabiliza-se pelo tratamento do risco, até que o mesmo seja transformado em residual, incluindo seu monitoramento pós tratamento. Porém a pessoa ou entidade apenas gere o risco, não se responsabilizando por quaisquer problemas legais que possam estar atrelados ao risco. Esse papel é atribuído a entidade.

Art. 2º Com o escopo da garantia dos objetivos estratégicos, bem como a perpetuidade da organização, o Gerenciamento de Riscos Corporativos – GRC possui, de acordo com a ISO 31000, onze princípios que norteiam a efetividade de ações. O SESI/RR fará o uso desses princípios para tratar riscos, pois guiam as ações previstas na Política de Gerenciamento de Riscos:

- Cria Valor;
- Parte integrante dos processos organizacionais;
- Parte da tomada de decisões;
- Aborda explicitamente a incerteza;
- Sistemática, estruturada e oportuna;
- Baseada nas melhores informações disponíveis;
- Feita sob medida;
- Considera fatores humanos e culturais;
- Transparente e inclusiva;
- Dinâmica, interativa e capaz de reagir a mudanças;
- Facilita a melhoria continua da organização;

Art. 3º A partir das diretrizes da ISO 31000, o Gerenciamento de Riscos Corporativos – GRC está estruturado em nove componentes, conforme expostos abaixo:

Ambiente Interno: É a base para todos os outros componentes da estrutura de controles, estabelecendo o desenho, o gerenciamento, o monitoramento e a disciplina dos administradores, funcionários, estagiários e prestadores de serviços alocados fisicamente nas dependências da entidade. O ambiente interno inclui a estrutura organizacional, os recursos humanos e físicos, a cultura e os valores do Posicionamento Estratégico (valores éticos e integridade), as competências e as habilidades.

Os objetivos estratégicos são definidos pelo CPGE, consoante com a Estratégia e a Atitude Perante ao Risco, o qual direciona o Nível de Risco nos processos e atividades executadas nos diversos objetivos presentes no Posicionamento Estratégico da entidade. Em função desses objetivos, são definidos conjuntos de Fatores Críticos e Planos de Ação para o seu cumprimento.

A estrutura de Gerenciamento de Riscos Corporativos – GRC assegura que a administração possui processos para definição de objetivos e que estes estejam alinhados com a estratégia em relação à Atitude Perante ao Risco.

Fixação de Objetivos: Os objetivos devem existir antes que a administração identifique as situações em potencial que poderão afetar a realização destes. O Gerenciamento de Riscos Corporativos – GRC assegura que o Comitê de Riscos adote um processo para identificar riscos e que os escolhidos propiciem suporte, alinhem-se com a missão da organização e sejam compatíveis com a Atitude Perante ao Risco.

Identificação dos Riscos: Os eventos em potencial que podem gerar consequências à organização devem ser identificados de acordo com o traçado nos objetivos presentes no Posicionamento Estratégico da entidade, uma vez que esses possíveis eventos, gerados por fontes internas ou externas, afetam a realização dos objetivos. Durante o processo de identificação de eventos, estes poderão ser diferenciados em riscos e oportunidades de melhoria, ou ambos. As oportunidades são canalizadas à Direção, que definirá as diretrizes estratégicas ou os objetivos.

Análise dos Riscos: A análise de riscos fornece uma compreensão sobre os riscos da entidade. Envolve a apreciação das causas e fontes de risco, suas consequências positivas e negativas, e também a probabilidade de que essas consequências possam ocorrer. Nessa etapa, o Comitê de Riscos deverá analisar todos os riscos identificados na etapa anterior, verificando quais são as consequências e probabilidade dos riscos, isso será insumo para a etapa posterior. O nível de risco é mensurado, mediante a matriz formada entre a probabilidade e consequência de cada risco traçado na identificação.

Avaliação de Riscos: A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto interno e externo for considerado. Compreendem a identificação e a análise dos riscos relevantes que comprometam o atendimento dos objetivos da entidade, formando uma base para determinar como os riscos devem ser gerenciados. O Comitê de Riscos deve avaliar os eventos de risco por seu impacto e sua probabilidade de ocorrência utilizando metodologias de mensuração, presentes na ISO 31010.

Nesse escopo, foi sugerida uma avaliação de riscos qualitativa, trabalhada numa matriz de Gerenciamento de Riscos Corporativos – GRC, proporcionando um mecanismo para tratamento de riscos. Consequentemente, é uma ferramenta de direcionamento dos esforços para tratar os riscos mais significativos por meio de uma estrutura de controles internos, alinhada aos objetivos presentes no Posicionamento Estratégico da entidade.

Tratamento ao Risco: Segundo a (ISO 31000, 2009 p. 19) "o tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes".

A implementação dos planos de ação para tratamento dos riscos compreende atividades específicas que visam transformar quaisquer riscos identificados em riscos residuais. Caso durante a avaliação o risco seja categorizado como trivial, este será monitorado e analisado criticamente, cuja periodicidade será definida pelo Comitê de Riscos, e monitorada pelo CPGE.

Atividades de Monitoramento: As atividades de monitoramento compreendem políticas e procedimentos elaborados para assegurar que as diretrizes e os objetivos, definidos pela entidade para minimizar seus riscos, estão sendo observados nas atividades executadas. As atividades de monitoramento ocorrem em todos os níveis da entidade e abrangem atividades como aprovações, autorizações, limites de alçada, verificações, reconciliações, revisões de performance operacional, segurança de ativos e segregação de funções, e será executada pelo Controle Interno e avaliada pelo CPGE.

Comunicação e Consulta: A forma e o prazo em que as informações relevantes são identificadas, colhidas e comunicadas permitam que as pessoas cumpram com suas atribuições. Para identificar, avaliar e responder ao risco, a organização necessita das informações em todos os níveis hierárquicos. A comunicação eficaz ocorre quando esta flui na organização em todas as direções, e quando os empregados recebem informações claras quanto às suas funções e responsabilidades.

Monitoramento e Análise Crítica: O Controle Interno executa o monitoramento e documentação das entregas previstas pelos proprietários de risco. A análise crítica é executada pelo Comitê de Riscos, que realizará a leitura das entregas e referendará as ações

previstas no tratamento de riscos. As principais atividades de monitoramento incluem conciliações, acompanhamento de comunicações de agentes externos e internos, inventários, auto avaliações e verificação contínua, bem como a avaliação constante da matriz de Gerenciamento de Riscos Corporativos – GRC, com intuito de fortalecer ainda mais à entidade, em busca da melhoria contínua.

Art. 4º A análise de riscos envolve a apreciação dos riscos, suas consequências e a probabilidade de que essas consequências (impactos) possam ocorrer. As consequências são niveladas de leve, moderado a extremo. Seus impactos são categorizados em baixo, médio e alto. Os riscos são analisados mediante o cruzamento desses dados, com intuito de gerar o Nível de Risco.

Pode ser executada mediante quaisquer ferramentas disponíveis na ISO 31010. O SESI/DR-RR elegeu a matriz de probabilidade x consequência para resultar seu nível de risco, da seguinte forma:

	Extremo = 5	Alto = 4	Moderado = 3	Baixo = 2	Irrelevante = 1
Quase Certo = 5	Intolerável = 10	Intolerável = 9	Importante = 8	Significante = 7	Moderado = 6
Muito Provável = 4	Intolerável = 9	Importante = 8	Significante = 7	Moderado = 6	Tolerável = 5
Pouco Provável = 3	Importante = 8	Significante = 7	Moderado = 6	Tolerável = 5	Trivial = 4
Improvável = 2	Significante = 7	Moderado = 6	Tolerável = 5	Trivial = 4	Insignificante = 3
Raro = 1	Moderado = 6	Tolerável = 5	Trivial = 4	Insignificante = 3	Insignificante = 3

Art. 5º A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento.

Compara o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado. Os critérios estipulados foram estipulados dessa forma:

ANÁLISE	CRITÉRIO
INSIGNIFICANTE	Não requer ação específica de tratamento. É considerado risco residual apenas pelo processo de análise. Monitorar anualmente e comparar com série histórica

TRIVIAL	Identificado, deve ser controlado periodicamente a fim de se evitar o aumento de sua criticidade. Não requer ação específica de tratamento. É considerado risco residual apenas pelo processo de análise. Monitorar anualmente e comparar com série histórica
TOLERÁVEL	Devem ser feitas considerações sobre uma solução de custo mais eficaz ou melhorias que não imponham uma carga de custos adicionais. Requeridas comprovações periódicas da eficácia das medidas de controle. Monitorar anualmente e comparar com série histórica
MODERADO	Devem ser determinados os investimentos necessários. O tratamento deve ser implementado dentro de um período de tempo definido. Quando o risco moderado está associado a consequências altamente prejudiciais, pode ser necessária uma avaliação adicional para estabelecer mais precisamente a probabilidade do dano, como base para determinar a necessidade de melhores controles operacionais. Monitorar anualmente e comparar com série histórica.
SIGNIFICANTE	Devem ser determinados os investimentos necessários. Monitorar anualmente e comparar com série histórica. Há necessidade de controlar o risco a fim de não prejudicar os objetivos que estão em execução.
IMPORTANTE	Devem ser determinados os investimentos necessários. O projeto deve ser reavaliado até que o risco tenha sido tratado. Pode ser que haja a necessidade de recursos consideráveis para realizar o tratamento, que não estavam previstos no projeto inicial. Caso o risco envolva um trabalho em execução, deve ser tomada uma ação urgente para tratamento. Monitorar e comparar com série histórica.
INTOLERÁVEL	Não deve ser começado, nem continuado o trabalho até que se trate o risco. Se não é possível tratar o risco, devido a recursos limitados, deve ser desdobrado para sofrer reavaliação ou eliminado. Monitorar comparar com série histórica.

Art. 6º O tratamento de riscos envolve a seleção de uma ou mais opções para tratar os riscos e a implementação dessas opções. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes.

Alternativas para Tratamentos dos Riscos:

- Redução da probabilidade;
- Redução da consequência;
- Redução da probabilidade e consequência;
- Remoção da fonte de risco, se possível;
- Exploração, se o risco for positivo;

- Compartilhamento;
- Retenção, por evidência consciente e embasada;
- Não realizar.

Art. 7º A Comunicação de Riscos segue um padrão uniforme, onde todas as partes interessadas sejam diretamente envolvidas. Convém que a comunicação seja parte integrante do Gerenciamento de Riscos Corporativos – GRC, e a cada evolução dos tratamentos previstos seja amplamente divulgada, mediante proposta de comunicação do proprietário do risco e deferida via Comitê de Riscos.

A formulação das entregas poderá ser acompanhada via CPGE e deferida via Subcomitê de Riscos, mediante a construção de uma planilha com as seguintes considerações:

- Risco Nrº;
- Quem recebe a informação?
- O que recebe de informação?
- Como recebe a informação?
- Quando recebe a informação?
- Como responde?
- Como devolve?
- Quem recebe devolução?
- Como recebe a devolução?
- O que faz com a entrega?
- Como faz a entrega?
- Para quem envia a entrega?

Art. 8º O comitê de crises é uma estrutura formada para gerir riscos tempestivos, oriundos de casos fortuitos ou forças maiores, que sejam caracterizados de alto impacto, advindos de eventos políticos, sociais, econômicos, legais, ambientais, tecnológicos ou de natureza interna, que possuam consequências relevantes à imagem da organização.

Este é constituído apenas em eventos dessa natureza.

Tal comitê é regido pela presente Instrução Normativa, com participação incisiva da direção, comunicação e gestores, a fim de apresentar soluções para tratamentos céleres e efetivos.

O comitê deverá:

- Escrever os procedimentos e dar alternativas de como tratar o evento imediatamente;
- Executar o fluxo de como tratar cada evento de crise na empresa e fora dela;
- Fazer rapidamente o levantamento de investimentos, se necessário;
- Resolver a crise.

Quando o risco gerado pelo evento se tornar residual, será inserido na base histórica do CPGE, e o comitê de crises é dissolvido.

Art. 9º Das responsabilidades:

Superintendência

- Definir e responsabilizar o mandato e comprometimento da estrutura de riscos, presente na ISO 31000: Assegurar recursos para tratamento de riscos, definir e aprovar a Política de Gestão de Riscos, assegurar que a cultura da organização e a Política de Gestão de Riscos estejam alinhadas e alinhar os objetivos do Gerenciamento de Riscos Corporativos – GRC com os objetivos e estratégias da organização.

CPGE

- Definir a estratégia da entidade para atendimento de seus objetivos de negócio;
- Definir o nível de atitude perante ao risco na condução dos negócios;
- Aprovar a Política de Riscos Corporativos, assim como suas revisões;
- Referendar os relatórios de controles internos e da gestão da Matriz de Gerenciamento de Riscos Corporativos – GRC;
- Aprovar a metodologia a ser utilizada para condução do processo de Gerenciamento de Riscos Corporativos – GRC, utilizando a ISO 31010 para definição de forma mais adequada de avaliação de riscos;

- Analisar e propor sugestões para o aperfeiçoamento dos processos de Gerenciamento de Riscos Corporativos – GRC;
- Apontar os integrantes do Subcomitê de Riscos;
- Apontar o líder do Comitê de Crises;
- Gerir os relatórios do monitoramento da gestão da Matriz de Gerenciamento de Riscos Corporativos – GRC e referendá-las com a Superintendência;
- Efetuar outras análises que entender necessárias;
- Prover plano de comunicação adequado, divulgado às partes interessadas.
- Reavaliar periodicamente a adequação da estratégia de monitoramento e análise crítica de novos riscos da entidade;
- Validar os relatórios dos proprietários de risco desenvolvido na matriz de Gerenciamento de Riscos Corporativos – GRC;

Controle Interno

- Avaliar o cenário macroeconômico e seus efeitos, em termos de risco, sobre os mercados em que a entidade atua;
- Gerir ações do Comitê de Crises (agendar entrevistas, controlar relatórios, gerir recursos)
- Monitorar os processos chaves e críticos, verificando, através de suas revisões periódicas, se os controles praticados pelo gestor atendem às necessidades de controle do processo;
- Informar a Direção Regional sobre os resultados dos planos de ação estabelecidos para cada um dos riscos identificados nos processos;
- Reportar aos Gestores as falhas observadas, oferecendo recomendações para saná-las;
- Salvaguardar os ativos de prejuízos decorrentes de fraudes ou de erros não intencionais;
- Intensificar ações que promova a melhoria da gestão de riscos do SESI-DR/RR;

- Proteger os ativos, ajudando a gestão na condução ordenada do negócio da Instituição;

- Prevenir antecipadamente o acontecimento de erros, desperdícios, abusos, práticas antieconômicas e fraudes;

- Propiciar informações oportunas e confiáveis, inclusive de caráter administrativo e operacional, sobre os resultados e efeitos atingidos;

- Apoiar a implementação de programas, projetos, atividades, sistemas e operações, visando à eficiência, eficácia e economia de recursos.

- Gerir recursos para o tratamento de Riscos;

- Avaliar o cumprimento – por todas as áreas do SESI RR, em suas operações realizadas – das políticas, diretrizes, normas e procedimentos corporativos ou específicos, com vistas à salvaguarda do patrimônio, à confiabilidade dos sistemas e à fidedignidade da aferição das informações orçamentárias, contábeis e financeiras, apontando para possíveis riscos, monitorando ainda, a integridade dos relacionamentos da casa, colaboradores, clientes e fornecedores do SESI/DR-RR.

Comitê de Riscos

- Analisar as políticas de risco corporativo, assim como quaisquer revisões, submetendo-a a aprovação ao CPGE;

- Acompanhar de forma sistemática o Gerenciamento de Riscos Corporativos – GRC com o objetivo de garantir sua eficácia e o cumprimento de seus objetivos;

- Executar o Processo de Avaliação de Riscos;

- Operar ações do Comitê de Crises;

- Prover monitoramento e análise crítica de maneira contínua os riscos residuais da matriz de Gerenciamento de Riscos Corporativos – GRC e incluir na matriz a identificação, análise e avaliação de novos riscos observados, consoantes ao desenvolvimento dos processos internos, promovendo o atingimento de metas propostas no Mapa Estratégico vigente;

- Validar a inserção de riscos inerentes à operação da entidade para os processos de risco, levando em consideração sua relevância;

- Contribuir para elaboração do relatório de riscos corporativos;

- Propor à Diretoria o nível de Atitude Perante ao Risco da entidade.

Dê ciência e cumpra-se.

Boa Vista – RR, 23 de julho de 2019.

Rivaldo Fernandes Neves
Diretor Regional do SESI/RR.