Política de Gerenciamento de Risco Operacional

SUMÁRIO

1. DECLARAÇÃO

A Diretoria Zipdin SCD aprova a presente política de estrutura de gerenciamento de risco operacional, em ata de reunião da Diretoria de 30/04/2020, e vem divulgá-la no site da instituição em conformidade com o artigo 56 da Resolução CMN nº 4.557/2017.

A presente política foi elaborada nos termos da Resolução CMN nº 4.557/2017.

2. ESTRUTURA DE GERENCIAMENTO DE RISCO OPERACIONAL

2.1 Estrutura ZIPDIN SCD

• Diretoria de Riscos e Capital

Responsável pela Supervisão do desenvolvimento, da implementação e do desempenho da estrutura de gerenciamento de riscos, incluindo seu aperfeiçoamento.

Também realiza a atividade de adequação à RAS e aos objetivos estratégicos da instituição, das políticas, dos processos, dos relatórios, dos sistemas e dos modelos utilizados no gerenciamento de riscos;

Capacitação dos integrantes da unidade específica, acerca das políticas, dos processos, dos relatórios, dos sistemas e dos modelos da estrutura de gerenciamento de riscos, mesmo que desenvolvidos por terceiros;

Participação no processo de tomada de decisões estratégicas relacionadas ao gerenciamento de riscos e, quando aplicável, ao gerenciamento de capital, auxiliando a Diretoria.

• Área de Risco

É responsável por manter a matriz de riscos operacionais com a avaliação da classificação dos eventos de riscos potenciais e da exposição (qualitativa/ quantitativa). Também coordena a coleta de informações para o gerenciamento de riscos operacionais, avalia a solução proposta para tratamento da causa raiz de perdas operacionais relevantes, acompanha as providências tomadas e os planos de ação para mitigação dos riscos, interagindo com as áreas envolvidas.

Também é de sua responsabilidade a elaboração de relatórios de Risco Operacional e para a Diretoria.

• Auditoria Interna

Responsável por examinar periodicamente os processos e controles relativos ao gerenciamento dos riscos operacionais.

• *Compliance*

Área responsável por assegurar a atualização das políticas, manuais e normais internas em conformidade com as mudanças na legislação, supervisionar o cumprimento destas e comunicar eventuais deficiências à Diretoria.

• Processos

É responsável por: elaborar e manter atualizado o mapeamento das atividades e elaborar os procedimentos em conjunto com as áreas; identificar e sinalizar riscos potenciais evidenciados nos processos para a elaboração da matriz de riscos; analisar os Boletins de Ocorrência, implementando planos de ações corretivas em conjunto com as áreas organizacionais; analisar causa raiz dos incidentes e propor ações preventivas; e identificar os riscos potenciais de novos produtos e serviços.

• Áreas envolvidas com atividades operacionais

Responsáveis por registrar incidentes ocorridos em suas atividades e identificar novos riscos potenciais.

2.2 Estrutura de Tecnologia da Informação

A Zipdin mantém uma estrutura de governança de TI visando assegurar a integridade, a segurança e a disponibilidade dos dados e dos sistemas de informação utilizados, em conformidade com a Política da Segurança da Informação.

A Diretoria de TI é responsável pela gestão dos serviços de Tecnologia da Informação.

A área de Processos e Produtos é responsável por elaborar e manter atualizado o mapeamento dos processos da empresa.

2.3 Gerenciamento integrado de riscos

Contempla as estruturas de gerenciamento contínuo e integrado de

riscos de crédito, mercado, operacional, liquidez, socioambiental e demais riscos relevantes e do gerenciamento contínuo de capital, alinhada às estratégias de longo prazo definidas pela Alta Administração.

Para a plena efetividade desta política, as ações tomadas encontram-se em conformidade com a Resolução 4.553/17, do CMN, que definiu modelo de segmentação 5 (S5) para o Sistema Financeiro.

Para atender às exigências regulamentares, a estrutura de gerenciamento de Riscos é compatível com a natureza de suas operações, com a complexidade dos produtos e serviços oferecidos, e proporcionais à dimensão de sua exposição aos riscos.

3. DEFINIÇÕES DO RISCO OPERACIONAL

O Risco Operacional é definido como a possibilidade de ocorrência de perdas resultantes direta ou indiretamente de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas e sistemas.

A definição de risco operacional também inclui o risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, bem como a sanção em razão de descumprimento de dispositivos legais e a indenização por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

Para fins desta política, são considerados como riscos operacionais, além de outros, os eventos de risco associados a:

I. Fraudes internas: possibilidade de adulteração de controles, descumprimento intencional de normas, vazamento de informação privilegiada, divulgação intencional de informações incorretas, desvio de valores e quaisquer outros comportamentos fraudulentos por parte de colaboradores e/ou prestadores de serviços;

II. Fraudes externas: ações intencionais executadas por entidades externas, pessoas físicas ou jurídicas, com o objetivo de lesar as instituições, mediante acesso aos sistemas de informação, documentos, falsificações, furtos, roubos e atos de vandalismo;

III. Falha humana: decorrente de equívoco, omissão, distração ou

negligência de colaboradores ou terceiros contratados para a execução de atividades operacionais;

IV. Demandas trabalhistas: descumprimento de cláusulas dos contratos de trabalho e de normas previstas na CLT – Consolidação das Leis do Trabalho, Decreto-Lei n° 5.452, de 01/05/1943, pagamento incorreto de verbas rescisórias e/ou alto número de reclamações trabalhistas;

V. Segurança deficiente do local de trabalho: instalações e equipamentos em desacordo com as normas vigentes e/ou alto índice de acidentes de trabalho;

VI. Práticas inadequadas relativas a clientes, produtos e serviços: formalização de negócios em desacordo com as respectivas normas ou manuais internos, cláusulas contratuais, normas legais e/ou que não atendam às necessidades demandadas pelos clientes;

VII. Danos a ativos físicos próprios ou de terceiros: danos causados por vandalismo, desastres ou fenômenos naturais, como por exemplo, tempestades, inundações e/ou vendaval;

VIII. Interrupção das atividades da instituição: danos causados por grave falta de energia, sabotagem e/ou falha nos servidores e estações de trabalho;

IX. Falhas em sistemas ou infraestrutura de tecnologia da informação: qualquer descontinuidade das atividades apoiadas por serviços tecnológicos, motivadas por falta de meios seguros de acesso, falhas de manutenção dos sistemas, erros na preparação de backups, falta de proteção de firewalls, inadequação de sistemas operacionais e aplicativos e/ou impossibilidade de recuperação de dados por queda de energia ou quebra de equipamentos;

X. Falhas na execução, no cumprimento de prazos e/ou no gerenciamento de atividades da instituição: comercialização de produtos em desacordo com as respectivas normas ou manuais internos e/ou normas legais;

XI. Risco legal associado à inadequação ou deficiência em contratos firmados pela instituição: possibilidade de questionamento jurídico na execução dos contratos firmados pela instituição e/ou sanções por parte de órgãos fiscalizadores em função da inobservância de leis, regulamentos e normas legais;

XII. Sanções em razão de descumprimento de dispositivos legais: penalidades administrativas ou financeiras motivadas pelo descumprimento de normas; e

XIII. Indenização por danos a terceiros decorrentes das atividades desenvolvidas pela instituição: indenizações pagas a clientes pelo não cumprimento da legislação pertinente aos produtos comercializados.

4. DIRETRIZES PARA O GERENCIAMENTO DO RISCO OPERACIONAL

A Zipdin possui Normativo para estabelecimento da Política de Risco Operacional, que apresenta uma estrutura de gerenciamento capacitada a identificar, avaliar, monitorar, controlar e mitigar os riscos operacionais aos quais a Renta esteja exposta, de acordo com a natureza e complexidade dos seus produtos, serviços, atividades, processos e sistemas. Para isso, a gestão dos Riscos Operacionais é norteada pelos seguintes princípios:

4.1 Princípio da Formalização

Todos os processos operacionais da Renta deverão estar mapeados e vinculados a normas, procedimentos e/ou manuais que regulem a sua execução, com clara definição das responsabilidades de todos os envolvidos.

A gestão dos riscos é formalizada e consolidada através da Matriz de Riscos e Controles, que tem como objetivo fornecer uma visão dos riscos aos quais as atividades e negócios da Renta estão sujeitos e os controles adotados para mitigar tais riscos, e através dos registros de eventos e exceções autorizadas,

como se segue:

- Matriz de Riscos e Controles - Permite à Gestora identificar, avaliar, tratar, controlar, consolidar e monitorar os riscos aos quais as atividades e negócios estão sujeitos. Tal matriz é periodicamente revisada, visando sua constante atualização. Nessa matriz os riscos são identificados e listados por área, juntamente aos controles envolvendo cada evento. Cada risco e controle trazem informações qualitativas permitindo, desta forma, a classificação de cada processo de acordo com os níveis

de exposição (alto, baixo ou médio), informando ainda o tipo de risco.

- Registros de Eventos - Considerados riscos efetivamente materializados e que podem resultar em perdas ou não. Riscos de menor nível de exposição podem ser autorizados através de Relatórios de *Compliance* ou em Estudo de Risco relativo a negócios específicos, desde que atendam às necessidades de flexibilização de padrões ou regras de negócios, porém devem acontecer dentro de parâmetros previamente definidos, com políticas internas e devidamente autorizadas por quem tenha poderes ou alçada. O registro dos eventos serve para acompanhar a conformidade dos processos e exposição aos riscos a que as atividades cotidianas estão sujeitas, ou mesmo nos quais venham a incorrer, para estabelecer e praticar controles internos e planos de ação que reduzam os respectivos riscos e corrijam as deficiências.

Estes procedimentos visam também à documentação e armazenamento de tais informações para formação de banco de dados sobre perdas operacionais. Tais informações permitirão à Companhia adotar abordagens e métodos mais eficazes na gestão do referido risco.

A alteração de procedimentos ou lançamento de novos produtos exigirá uma avaliação dos riscos operacionais vinculados, que se torna fundamental para o cumprimento do Princípio da Formalização.

4.2 Princípio da Disseminação

As normas e os procedimentos mencionados anteriormente devem estar acessíveis a todos os empregados e colaboradores, assim como o conceito de risco operacional. A área de Processos é responsável pela publicação e atualização de todos os normativos. Todos os processos internos foram mapeados e disponibilizados na forma de Manuais. A revisão dos normativos ocorre, no mínimo, uma vez a cada ano, por mudança de processo ou por demanda da diretoria.

4.3 Princípio da Atualização

A Política de Gerenciamento do Risco Operacional deverá ser objeto de permanente atualização, objetivando seu aperfeiçoamento com correções e melhorias.

4.4 Princípio da Avaliação

Manter instrumento para controle e comunicação dos riscos aos responsáveis pelos processos, fomentando o reporte de incidentes

operacionais para adequação dos controles internos resultando em planos de ação mitigatórias com correções e melhorias.

4.5 Princípio do Monitoramento

O monitoramento dos riscos é realizado não só com base na verificação dos controles executados, mas também pelo acompanhamento das perdas efetivadas, sejam financeiras eu não.

As ocorrências são verificadas, especialmente, com base nos registros contábeis que refletem falha operacional, como multas, demandas trabalhistas, etc.

O enquadramento das carteiras também está contemplado no processo de monitoramento, de forma a garantir a conformidade com as regras regulamentares.

5. CICLO DO GERENCIAMENTO DOS RISCOS OPERACIONAIS

- Planejamento: Avaliação dos riscos identificados e revisão dos processos internos de gestão de risco;
- Identificação e classificação: coleta das informações e classificação das ocorrências de acordo com severidade e impacto;
- Tratamento: tratamento das ocorrências com o gestor da área;
- Controle: acompanhamento dos planos de ação e proposta de melhora de processos e controles.

A observação dos eventos classificáveis como risco operacional tem a finalidade preventiva, mediante a verificação de indicadores chave de risco e a consequente proposta de aperfeiçoamento dos processos, e corretiva, que é a análise pós ocorrência do incidente, e sua potencialidade de perda financeira.

A área de riscos é o ponto central de controle para concentração das informações, sendo responsável pela coleta das fontes de informações geradas pelas áreas operacionais:

- Coleta de informações relevantes das áreas meio e fins, relativas aos Sistemas de Controles Internos (aspectos preventivos e corretivos);

- Relatório de chamados abertos pelo gestor da área (aspectos corretivos);

- Relatório de eventos de riscos, tratados pelo Plano de Continuidade de Negócios (aspectos corretivos);

- Perdas financeiras contabilizadas nas contas criadas de acordo com o COSIF (aspectos corretivos).

5.1 Avaliação qualitativa dos riscos

Após a identificação dos eventos, é iniciada a classificação dos riscos para priorização do tratamento dos mesmos. Para estabelecer níveis diferentes de risco, foi criada a matriz abaixo que define a exposição qualitativa do risco, como o resultado da probabilidade de ocorrer e do impacto causado por um evento.

		Impacto				
		Extremo	*Alto*	*Médio*	*Baixo*	*Irrelevante*
Probabilidade	*Quase Certa*	Alto	Alto	Alto	Médio	Médio
	Provável	Alto	Alto	Médio	Médio	Médio
	Possível	Alto	Médio	Médio	Médio	Baixo
	Improvável	Médio	Médio	Médio	Baixo	Baixo
	Rara	Médio	Médio	Baixo	Baixo	Baixo

5.2 Tratamento e controle dos riscos

Para controle dos riscos identificados, a Zipdin adota os índices chamados de Indicadores de Chave de Risco (ICR), sendo que essas classificações são baseadas nas disposições da Resolução nº 4.557/17:

- Fraudes internas;

- Fraudes externas;

- Falha humana;

- Demandas trabalhistas;

- Segurança deficiente do local de trabalho;

- Práticas inadequadas relativas a clientes, produtos e

serviços; • Danos a ativos físicos próprios ou de terceiros;

• Interrupção das atividades da instituição;

• Falhas em sistemas de tecnologia da informação;

• Falhas na execução, no cumprimento de prazos e/ou no gerenciamento de atividades da instituição;

• Risco legal associado à inadequação ou deficiência em contratos firmados pela instituição;

• Sanções em razão de descumprimento de dispositivos legais;

• Indenização por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

Estes indicadores servem como base para avaliação e mensuração da exposição, e priorização dos esforços em controles relacionados às ocorrências registradas anteriormente.

O tratamento imediato das ocorrências é feito pela área de processos em conjunto com os gestores das áreas envolvidas. Por ser uma atividade constante, o tratamento das ocorrências é imediato, garantindo que os riscos sejam mantidos sob controle, com a consequente minimização de potenciais perdas.

Nas situações em que a área de riscos identifica e classifica evento de risco com exposição “Alta”, o fato é informado imediatamente ao conhecimento da Diretoria de Riscos e, dependendo de suas características e efeitos, ao Diretor Presidente, para a adoção de medidas corretivas urgentes.

5.3 Relatório do Risco Operacional

O relatório de Risco Operacional é elaborado anualmente e está em conformidade com o inciso X do artigo 7º da Resolução CMN nº 4.557/17.

5.4 Relatório do Sistema de Controles Internos

São elaborados semestralmente os relatórios do Sistema de Controles Internos em cumprimento da Resolução CMN nº 2.554/98 e da Circular Bacen nº 3.467/09.

6. PLANO DE CONTINUIDADE DOS NEGÓCIOS

O Plano de Continuidade dos Negócios ("PCN") faz referência ao conjunto de ações e procedimentos a serem adotados para suportar adversidades durante a ocorrência de situações de contingência em geral, com vistas a manter o funcionamento da empresa e a continuidade dos seus negócios.

O objetivo deste Plano é prevenir e minimizar os impactos causados pela interrupção dos processos de negócios e viabilizando a ativação de processos alternativos, nos tempos previamente acordados, e garantir o retorno à normalidade.

Todos os processos que fazem parte do PCN são objeto de testes constantes, alguns diariamente, pela área de TI e com acompanhamento periódico das áreas de negócio específicas e da área de Controles Internos.

Em eventos de indisponibilidades, total ou parcial, do escritório principal, todos os colaboradores podem trabalhar no formato home office, acessando todas as informações necessárias à continuidade das operações.

Periodicamente é realizada análise de cenários de alta severidade com base na matriz de indicadores chaves de riscos, para implementar/revisar novos controles e minimizar eventuais perdas, observando o artigo 33, inciso VI da Resolução CMN nº 4.557/17.

Também são feitos testes e revisões dos planos de continuidade de negócios periodicamente, com os respectivos relatórios, em conformidade com o § 2º artigo 20 da Resolução CMN nº 4.557/17.

7. DIRETRIZES GERAIS

O descumprimento das disposições dos órgãos reguladores sujeita os administradores e colaboradores da companhia a sanções de penalidades administrativas.

Os infratores estão sujeitos à aplicação das medidas disciplinares previstas nos normativos da empresa e sua abrangência.

O disposto acima se aplica, imediatamente, para toda a companhia a partir da data de sua publicação.

8. REVISÃO DA POLÍTICA

As políticas e procedimentos estão publicados na forma de Política e ao alcance de todos os colaboradores e devem ser objeto de permanente atualização, objetivando seu aperfeiçoamento com correções e melhorias. A revisão dos normativos ocorre, no mínimo, uma vez a cada ano, por mudança de processo,
ou por demanda da Diretoria para adequação dos processos, conforme estabelecido na Resolução CMN nº 4.557/17.