POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS

OBJETIVO

Esta política tem por objetivo estabelecer, na Bitcoin To You, princípios, diretrizes e responsabilidades a serem observados no processo de gestão dos riscos corporativos, de forma a possibilitar a adequada identificação, avaliação, tratamento, monitoramento e comunicação.

ABRANGÊNCIA

Esta política aplica-se a todos os colaboradores e prestadores de serviços da Bitcoin To You na gestão dos riscos que impactam o seu ambiente de forma corporativa.

DIRETRIZES

A Bitcoin To You está comprometida em manter um modelo de governança robusto e integrado visando assegurar, para o benefício de seus públicos de interesse (clientes, fornecedores, colaboradores, sociedade, governo, investidores, etc.), a concretização de seus objetivos empresariais cumprindo suas responsabilidades com diligência e prestação de contas.

A Bitcoin To You entende o gerenciamento de riscos corporativos como sendo um componente fundamental desse compromisso. O gerenciamento de riscos coporativos é um processo contínuo, transparente e de responsabilidade de todos os colaboradores da organização em todos os níveis. Cada um é responsável por conhecer os Riscos na sua área de atuação e geri-los de acordo com os conceitos, diretrizes e direcionamentos contidos nesta política e em seus documentos complementares.

Dessa forma, a Bitcoin To You busca estabelecer as regras para gerenciamento de risco, baseada nas melhores práticas e regulações existentes, por meio da segregação das linhas de defesa e pelo monitoramento dos controles internos.

São consideradas “linhas de defesa” as segregações de funções, papéis, responsabilidades, áreas e práticas com o objetivo de mitigar a materialização dos riscos que possam acarretar prejuízos à Empresa.

1. Primeira linha de defesa:

A primeira linha de defesa é a responsável direta por gerir, identificar, monitorar, eliminar e/ou reduzir a materialização dos riscos. Tais defesas são comumente relacionadas às funções, práticas e áreas que mantém os processos operacionais da Bitcoin To You. Desta forma, esta linha de defesa possui os objetivos:

- Identificar, avaliar, controlar, eliminar e/ou reduzir os riscos;
- Criar ações que permitam a melhor gestão e controle para o tratamento dos riscos;
- Manter os controles internos diligentes; e
- Informar potenciais prejuízos da organização.

2. Segunda linha de defesa

A segunda linha de defesa da Bitcoin To You fica responsável pela controle e monitoramento dos níveis de riscos, de forma a assegurar que estejam dentro do nível permitido estabelecido. Desta forma, esta linha de defesa possui os objetivos:

- Garantir a efetivação e implementação da estrutura de gerenciamento de riscos;
- Fornecer orientação sobre as práticas a serem adotadas para se garantir eficiência na gestão de riscos;

- Garantir que o estabelecimento de limites e alçada de aprovação serão seguidas e cumpridas;
- Gerenciar e monitorar os riscos e perdas operacionais;
- Gerenciar e monitorar a eficiência obtida nos controles internos e ações de mitigação de riscos;
- Prover visibilidade aos gestores quanto a situação do ambiente de controle e riscos.

3. Terceira linha de defesa:

A terceira linha de defesa da Bitcoin To You é a responsável pela avaliação independente dos controles internos e riscos à alta administração da empresa. Desta forma, esta linha de defesa possui os objetivos:

- Auditar e monitorar os processos e controles internos de forma independente.
- Realizar e criar avaliações sobre que permitam medir a eficiência do gerenciamento de riscos e dos controles internos.

REGRAS PARA GERENCIAMENTO DE RISCOS

A estrutura de gerenciamento de risco deve ser segregada por linhas de defesa, capaz de avaliar periodicamente os processos, práticas e controles com o objetivo de identificar e mensurar vulnerabilidades que podem acarretar perdas e, consecutivamente, impactar os objetivos de negócio.

Os processos devem possuir atividades de controles que assegurem que seus riscos sejam conhecidos, controlados e mitigados adequadamente.

A mensuração do risco deve considerar a exposição à vulnerabilidade e ao impacto, com base nos limites descritos abaixo.

1. Identificação da vulnerabilidade

O primeiro passo para eficiência no gerenciamento de riscos é a identificação do nível de vulnerabilidade do risco. Para tanto os riscos devem ser controlados, posteriormente identificados, avaliados, documentados e formalizados conforme o nível de vulnerabilidade para que possam ser tratados de forma correta.

2. Mensuração de vulnerabilidade

Para se medir a vulnerabilidade dos riscos, esses devem ser controlados, posteriormente identificados, avaliados, documentados e formalizados conforme o nível de vulnerabilidade evidenciado abaixo para que possam ser tratados de forma correta.

- **Baixo:** existência de controles internos eficazes para mitigação dos riscos.
- **Médio:** predominância de controles internos eficazes para mitigação dos riscos.
- **Alto:** poucos controles eficazes para mitigação dos riscos.
- **Extremo**: inexistência ou predominância de controles ineficazes para mitigação dos riscos.

3. Mensuração do impacto

A quantificação e controle do risco devem ser realizados com base no impacto gerado por ele sob as perspectivas financeiras, operacionais, reputacional e regulatório.

4. Impacto reputacional (perspectivas financeiras)

Um outro fato de mensuração de risco a ser levando em conta é o impacto do mesmo sob a perspectiva reputacional, pois afeta diretamente a empresa e consequentemente impacta financeiramente a Bitcoin To You. Nesse sentido a

escala de impacto na reputação da empresa para a mensuração do risco se estrutura da seguinte forma:

- **Baixo:** impacto irrelevante na reputação, em pequeno grupo de cliente e com rápida remediação.
- **Médio:** impacto mínimo na reputação, atenção da mídia local e reversíveis no curto prazo.
- **Alto:** poucos controles eficazes para mitigação dos riscos.
- **Extremo:** inexistência ou predominância de controles ineficazes para mitigação dos riscos.

5. Impacto regulatório

O impacto regulatório é avaliado com objetivo de prevenir riscos de multas, sanções, penalidades e outros derivados de normas regulamentadoras da atividade. Embora não há normas específicas para a atividade desenvolvida pela Bitcoin To You, ela segue a melhor formatação legal tutela por analogia o exercício de sua atividade. Nesse sentido a escala de impacto regulatório a ser considerada para a mensuração do risco é:

- **Baixo:** notificações legais que não resultam em penalidades ou multa.
- **Médio:** notificações legais que resultaram em aplicação de multas ou sanções não significativas.
- **Alto:** notificações legais que resultaram na aplicação de multas ou sanções significativas que não impactam a continuidade das operações de negócio.
- **Extremo:** exposição e grande tendência a notificações legais com geração de penalidades, devido a inexistência ou predominância de controles ineficazes para mitigação dos riscos.

6. Tratamento e monitoração

Para tratar os riscos deve-se atentar ao nível de exposição e prioridade. Desta forma, as medidas abaixo podem ser adotadas como tratamento do risco:

- **Evitar:** descontinuar atividades, produtos, serviços, negócios, práticas ou processos que acarretam os riscos identificados.
- **Reduzir:** adotar medidas ou ações para reduzir e/ou eliminar a vulnerabilidade ou impacto do risco identificado.
- **Compartilhar:** transferir a vulnerabilidade ou impacto para terceiros.
- **Aceitar:** não há o que fazer e/ou nenhuma medida é adotada.

7. Prazo de tratamento

Os responsáveis pelo risco, gestores da primeira linha de defesa, devem realizar o tratamento do risco conforme o nível de exposição e dentro dos prazos abaixo:

- **Baixo:** em até 360 dias após a identificação.
- **Médio:** em até 180 dias após a identificação.
- **Alto:** em até 60 dias após a identificação.
- **Extremo:** imediatamente limitado em até 30 dias após a identificação.

Quando se trata de riscos que possuem impactos regulatórios, esses devem ser tratados dentro dos prazos estipulados pelos órgãos reguladores e lei, por exemplo: notificações do COAF, notificações da Receita Federal e outros.

8. Alçada de aprovação

Para garantir a eficiência no tratamento dos riscos, estes devem ser aprovados conforme alçada abaixo.

- **Risco baixo:** colaborador responsável pelo processo e/ou atividade;
- **Risco médio:** coordenador do setor e/ou departamento;

- **Risco alto:** coordenador do setor e/ou departamento em conjunto com diretores.
- **Risco extremo:** sócio administrador.

DISPOSICÕES GERAIS

Considerando a complexidade em gerenciar riscos corporativos, as particularidades do negócio e suas operações, bem como sua estrutura operacional, esta política poderá ser complementada por procedimentos específicos (normas, procedimentos e instruções de trabalho) quando aplicável e requerido.