Política de Seleção de Exchanges e Demais Serviços de Criptoativos

Pandhora Investimentos Ltda.

Março, 2023

SUMÁRIO

1. OBJETIVO ---------- 3

2. DEFINIÇÃO ---------- 3

3. ESCOPO REGULATÓRIO ---------- 3

3.1. *MONEY SERVICE BUSINESS* ---------- 4

3.2. *BITLICENSE* ---------- 4

3.3. DEMAIS LOCALIDADES ---------- 5

4. SEGURANÇA DE SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO ---------- 5

4.1. ISO 27001 ---------- 5

4.1. SOC 2 TIPO 2 ---------- 6

5. CUSTÓDIA ---------- 7

6. EXCEÇÕES ---------- 7

7. ATUALIZAÇÃO E REVISÃO ---------- 7

1. OBJETIVO

A Presente Política de Seleção de Exchanges e demais Serviços de Criptoativos ("Política") visa estabelecer as regras gerais para os processos de contratação de *Exchanges* e/ou serviços similares para os fundos da gestora que investem diretamente em criptoativos.

Esta Política trata sobre as diretrizes para as contratações de terceiros que oferecem serviços relacionados ao tema e é pautada nas boas práticas comerciais e de gestão, sendo um complemento às normas e políticas internas da Gestora, inclusive o Código de Ética e Manual de Controles Internos.

Esta Política utiliza como referência principal o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, bem como demais normas regulatórias e autorregulatórias aplicáveis ao mercado tradicional. Além disso, dado a natureza dos ativos, informações consideradas necessárias foram incluídas.

2. DEFINIÇÃO

Para os fins da presente Política, considera-se *Exchange,* empresa individual (pessoa jurídica) ou sociedade empresária (sociedade anônima, limitada etc.) de conversão de moedas fiduciárias por criptoativos e/ou custódia destes, ou que preste serviço envolvendo a posse e/ou troca destes ativos.

3. ESCOPO REGULATÓRIO

Os critérios foram baseados em boas práticas vistas principalmente no exterior e regulamentações de alguns países ou partes autônomas dentro deles. Nesta seção serão abordadas as principais que são utilizadas como critérios.

3.1. *Money Service Business*

Oferecida pela Rede de Combate a Crimes Financeiros (*Financial Crimes Enforcement Network*, ou *FinCEN*), traz diversas obrigações às companhias consideradas *MSBs*, como por exemplo:

• Identificação de pessoas que detenham propriedade ou o controle do *MSB*.

• Definição de uma política formal de Prevenção a Lavagem de Dinheiro e Financiamento de Terrorismo. Com documentação, treinamento, auditoria independente e nomeação de um *Compliance Officer*.

• Políticas e processos rígidos de identificação e verificação de clientes.

• Preenchimento e envio de Relatórios de Atividades Suspeitas (*Suspicious Activity Reports – SARs*) para transações suspeitas.

• Preenchimento e envio de Relatóriso de Transação de Moedas (*Currency Transaction Reports – CTRs*) para movimentações acima de 10 mil dólares.

• Manutenção de um histórico de 5 anos para conversões de moedas acima de 1 mil dólares e transferências acima de 3 mil dólares.

Essa licença é considerada um pré-requisito, a não ser para casos descritos na seção de exceções. Sendo verificada anualmente a validade da licença no próprio site da *FinCEN*.

3.2. *BitLicense*

Oferecido pelo Departamento de Serviços Financeiros do Estado de Nova Iorque (*NYDFS*) a todas às Instituições Financeiras que desejam operar em seu território. Esta licença é específica para *Exchanges* e complementa o *MSB* com uma série de novas exigências, como:

• Envio de Demonstrativos Financeiros independentemente auditados, incluindo Balanço Patrimonial, Demonstrativo de Resultados do Exercício, seguros e serviços bancários.

• Requerimentos de Capital definidos a critério próprio do *NYDFS*.

• Reservas completas dos ativos custodiados, com proibição da utilização destes para outras operações.

• Fotos e impressões digitais de todos os funcionários com acesso aos ativos dos clientes.

• Nomear um *Chief Information Security Officer* qualificado e realização anual de testes de penetração.

• Documentação e implementação de um Plano de Continuidade de Negócios e Recuperação de Desastres, rodados independentemente anualmente.

• Auditorias independentes do *NYDFS* a critério próprio.

A *BitLicense* é considerada a mais rigorosa em termos de operações, e é considerada por nós desejável, porém não obrigatória.

3.3. Demais Localidades

Além da *FinCEN*, a *Fintrac* do Canadá também emite uma licença de *MSB*. Outros órgãos também possuem licenças mais genéricas para funcionamento de entidades financeiras, como a *FCA* do Reino Unido e a *ASIC* da Austrália. Portanto, quanto mais licenças, melhor para a avaliação da *Exchange*.

4. Segurança de Sistemas de Tecnologia da Informação

Dado a natureza digital dos criptoativos, um dos riscos inerentes é o de roubo via *hacking.* Portanto, saber se a instituição possui sistemas minimamente seguros é fundamental para a decisão de alocação. Para a Pandhora os principais selos de aprovação no sentido de cyber segurança são os seguintes:

4.1. ISO 27001

ISO/IEC 27001 é um padrão para sistema de gestão da segurança da informação (*ISMS - Information Security Management System*) publicado em outubro de 2005

pelo *International Organization for Standardization e pelo International Electrotechnical Commission*. O seu nome completo é ISO/IEC 27001- Tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação - requisitos, mais conhecido como ISO 27001.

Esta norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. Um SGSI introduzido em alguma entidade possui o intuito de reduzir a probabilidade e/ou o impacto provocado por algum tipo de incidente de segurança da informação. A especificação e implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, exigências de segurança, os processos empregados e o tamanho e estrutura da organização.

4.1. SOC 2 Tipo 2

Os SOC (Controles de Sistema e Organização) para Organizações de Serviço são relatórios de controle interno criados pelo *AICPA (American Institute of Certified Public Controls)*. Eles se destinam a examinar os serviços fornecidos por uma organização de serviço para que os usuários finais possam avaliar e resolver o risco associado a um serviço terceirizado.

Uma auditoria SOC 2 fornece aos clientes e partes interessadas de uma organização uma garantia sobre a adequação e eficácia de seus controles de dados, com base em sua conformidade com os critérios de serviços de confiança estabelecidos pelo *AICPA*. Esses critérios são divididos em quatro categorias: controles de acesso lógico e físico, operações do sistema, gerenciamento de mudanças e mitigação de riscos. O SOC 2 não é uma certificação, mas sim um exame dos controles de dados de uma organização e a opinião de um terceiro credenciado sobre a adequação desses controles.

Importante ressaltar que estamos falando do SOC 2 Tipo 2, já que o SOC 1 examina apenas os protocolos de relatórios financeiros de uma empresa. E que o Tipo 1 é

uma avaliação pontual dos controles, já o Tipo II é uma avaliação da eficácia dos controles ao longo de um período, normalmente seis meses ou mais.

Para a Pandhora é desejável que o prestador possua pelo menos um dos dois de forma verificável.

5. CUSTÓDIA

Um dos riscos do mercado cripto é a falência de *Exchanges* provocando o congelamento dos ativos, muitas vezes não sendo recuperados. Para reduzir tal risco, na Pandhora, decidiu-se por ter um custodiante regulado, a *Coinbase Custody*, que é uma entidade apartada da *exchange Coinbase*, regulada pelo Estado de NY através da *NYDFS – New York Departament of Financial Services*, mesmo regulador dos grandes bancos americanos.

O objetivo é manter mais de 90% dos ativos custodiados nela. Assim, as *exchanges* serão utilizadas apenas com a finalidade de *trading*, e os ativos serão enviados ao custodiante após a operação.

6. EXCEÇÕES

O mercado de cripto é novo, logo há muita concentração em determinados serviços que podem impactar as estratégias, um exemplo disso são os derivativos, que hoje estão concentrados na *Deribit*. Ela concentra mais de 90% do mercado de opções. Portanto, serviços assim são sujeitos a uma aprovação por exceção, mesmo não apresentando os certificados acima, desde que respeite a regra de custódia.

7. ATUALIZAÇÃO E REVISÃO

Esta Política de Seleção de *Exchanges* será revisada e atualizada pelo time de *Compliance* e Risco em parceira com o time de Gestão de Criptoativos, em periodicidade, no mínimo anual. Será atualizada, também, caso haja adoção de novos procedimentos ou adequação a novos normativos. A aprovação desta política é realizada pelo Comitê de *Compliance*.