Hashdex

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

SOMENTE PARA USO INTERNO

Este material foi elaborado pela Hashdex Gestora de Recursos Ltda. ("Hashdex" ou "Gestora") e não pode ser copiado, reproduzido ou distribuído sem prévia e expressa concordância desta.

# Hashdex

Ficha Técnica:

| | |
|---|---|
| Título: | Política de Segurança da Informação e Segurança Cibernética |
| Área responsável: | *Compliance* |
| Diretor responsável: | Bruno Ramos de Sousa |
| Descrição da Política: | Trata-se de Política de Segurança da Informação e Segurança Cibernética, como parte de seu dever fiduciário na execução de suas operações visando sempre as melhores condições para seus clientes. |
| Aplicação: | Todos os Colaboradores da Hashdex, conforme definição do Manual de *Compliance* da Gestora |
| Data de aprovação: | 12 de fevereiro de 2019 |
| Aprovado por: | Comitê de Risco e *Compliance* |
| Data da Última Atualização: | 31 de agosto de 2020 |

# 1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## 1.1 Introdução

A Política de Segurança da Informação ("Política") tem por razão o adequado gerenciamento das informações de posse temporária ou de propriedade da Gestora. Assim, deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A responsabilidade em relação à segurança da informação deve ser comunicada no início do vínculo com a Gestora, devendo os mesmos assinar o Termo de Responsabilidade e Confidencialidade, de forma manual ou eletrônica, salvo se permitido em lei, na forma do Anexo I a esta Política.

A área de *Compliance* realizará a revisão e atualização desta Política periodicamente ou sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de *Compliance*.

## 1.2 Confidencialidade

Os Colaboradores deverão observar as regras de confidencialidade prevista na Política de Confidencialidade das Informações, constantes do Manual de *Compliance* da Gestora ("Manual"), inclusive no que refere ao conceito de "Informações Confidenciais".

Todo Colaborador a quem se conceda acesso a informações confidenciais deve ser identificado no nível da pessoa física (nos termos do idem 1.4, abaixo), e, nesta condição, respeitar todos os procedimentos determinados nesta e demais Políticas da Hashdex. Apenas pessoas autorizadas terão acesso a informação confidencial, e apenas na medida do necessário para a execução de suas atividades.

Caso um detentor de informação confidencial mude de função dentro da Hashdex na qual o acesso a tal informação não seja mais necessário, então o acesso do Colaborador será restringido pelo responsável de Tecnologia da Informação.

Da mesma forma, ato contínuo ao desligamento de um Colaborador, o acesso deste a todos os sistemas, informações e documentos da Hashdex será bloqueado.

## 1.3 Barreira de Controle de Informações

Os Colaboradores detentores de Informações Confidenciais ou Privilegiadas, em função de seus cargos ou atribuições na Gestora, devem estabelecer uma barreira de informações

para os demais Colaboradores. De forma não exaustiva, as seguintes condutas devem ser observadas:

- Os Colaboradores devem evitar circular em ambientes externos à Gestora com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, devendo essas cópias ser criptografadas ou mantidas através de senha de acesso;
- Os documentos descartados devem ser destruídos, de forma a garantir que informações relevantes não sejam repassadas a terceiros;
- O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico;
- As informações que possibilitem a identificação de um cliente da Gestora devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da Gestora ou do próprio cliente;
- Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes, etc; e
- Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos.

## 1.4 Identificação dos Detentores da Informação, Manutenção de Registros e *Logs*

O Diretor de *Compliance* deve manter o registro dos Colaboradores que detenham Informações Privilegiadas e/ou Confidenciais, com a indicação do tipo de informação detida, devendo informar aos demais Diretores da Gestora todas as Informações Privilegiadas que estejam em poder dos Colaboradores que possam significar restrição nas operações da Gestora.

Será atribuído a cada conta ou dispositivo de acesso a sistemas, bases de dados e qualquer outro ativo de informação, um responsável identificável como pessoa física, sendo que os usuários (*login*) individuais de Colaboradores internos serão de responsabilidade do próprio Colaborador e os usuários (*login*) de terceiros serão de responsabilidade do diretor da área contratante. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

Com relação ao monitoramento e auditoria do ambiente, a Gestora possui sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

A Gestora informa, ainda, que poderá tomar as seguintes medidas:

- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Diretor de *Compliance*;

- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade; ou
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.
- Instalar sistemas de rastreamento e monitoramento de estações móveis de trabalho com a possibilidade de remoção remota de todos os arquivos no caso de perda ou roubo do dispositivo.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas da Gestora e sujeitará o usuário às sanções administrativas e legais cabíveis, observado o disposto no item que trata de Sanções, constante do Código de Ética da Gestora.

Para fins de ilustração, segue uma lista não exaustiva de eventuais exemplos que podem ocasionar sanções: uso ilegal de software; introdução (intencional ou não) de vírus de informática; tentativas de acesso não autorizado a dados e sistemas; ou divulgação de informações sensíveis e/ou confidenciais da Gestora.

## 1.5 Proteção da Base de Dados

Os recursos computacionais da Gestora devem: (i) ser protegidos contra adulterações; e (ii) permitir a realização de auditorias e inspeções.

Todos os registros eletrônicos realizados pela Gestora deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que a Gestora atue em mercado regulado.

As informações mantidas em meios eletrônicos devem possuir polícias de backup periódicas e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso a essas bases deve ser limitado somente a pessoas autorizadas pela área de *Compliance*.

## 1.6 Vazamento de Informações Confidenciais

Os Colaboradores deverão comunicar à área de *Compliance* quaisquer casos de violações às normas de segurança da informação que tenham conhecimento. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Em caso de vazamento de informação confidencial, o Diretor de *Compliance* discutirá com o Comitê de Risco e *Compliance* (ou, se for o caso, com o Responsável pela Segurança Cibernética, qual o melhor plano efetivo de recuperação e medidas para minimizar e prevenir danos.

## 1.7 Testes e Treinamento de Segurança da Informação

A Gestora realizará testes periódicos de segurança para os sistemas de informações (sem se limitar a, mas em especial, para os meios eletrônicos), no mínimo anualmente, visando

reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

O treinamento sobre segurança de informação fará parte do treinamento inicial e periódico da Gestora, conforme previsto na Política de Treinamento do Manual, o qual deverá considerar, dentre outros, assegurar que todos os Colaboradores tenham conhecimento dos procedimentos e das obrigações aqui previstos, assim como minimizar a ocorrência de incidentes de segurança em função de problemas no uso, desvio de informações, fraudes e na interpretação das normas e procedimentos.

## 1.8 Política para Dispositivos Pessoais

Os Colaboradores deverão comunicar à área de *Compliance* sua opção por utilizar seus dispositivos pessoais (BYOD – *bring your own device*), como smartphones e laptops, para acesso à rede corporativa, sistemas internos e bancos de dados.

Os dispositivos BYOD devem ser constantemente monitorados pela Gestora. Esse monitoramento é importante para ter conhecimento de possíveis violações à política de segurança, incidentes e poder tomar ações preventivas.

A área de *Compliance* auditará o dispositivo, e poderá instalar ferramentas de monitoramento e remoção remota de informações (para caso de roubo ou perda do dispositivo) e somente aprovará seu uso se o Colaborador concordar em:

- Acompanhar treinamentos de segurança promovidos periodicamente pela área de *Compliance;*
- Aprovar a gestão de soluções móveis da Gestora, que contém, dentre seus principais termos, os seguintes pontos:
    - Ações para bloqueamento remoto,
    - Remoção completa de arquivos,
    - Restauração aos padrões de fábrica,
    - Monitoramento constante de atividades realizadas no dispositivo;
- Possuir disco rígido criptografado (para laptops);
- Possuir solução antivírus ou malware;
- Seguir os procedimentos definidos na seção 2.7.1 em casos de incidentes como roubo ou extravio dos dispositivos pessoais que possam ter sido usado para realizar qualquer tarefa relacionada a Gestora;
- Utilizar sempre a versão mais atualizada do sistema operacional e efetuar todas as atualizações do fabricante;
- Utilizar autenticação de múltiplos fatores (2FA) em todos os sistemas da Gestora;
- Não utilizar logins pessoais para qualquer tarefa relacionada à Gestora;
- Não emprestar o dispositivo para terceiros, inclusive membros da família;
- Não instalar aplicativos não oficiais ou não homologados pela Gestora;
- Evitar o uso de redes de Wi-Fi públicas;

- Nunca clicar em links ou abrir anexos de e-mails de fontes não confiáveis para evitar *phishing;*
- Retornar o dispositivo à área de Compliance, no caso de desligamento, para reconfiguração e limpeza de dados da Gestora;

# 2. POLÍTICA DE SEGURANÇA CIBERNÉTICA

## 2.1 Objetivo

A Política de Segurança Cibernética ("Política") tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética da Gestora. Assim, deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

A Política segue práticas de mercado, bem como está de acordo com as leis, regulamentação e autorregulação aplicáveis, incluindo o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros e o Guia de Cibersegurança de dez/2017.

## 2.2 Princípios

O objetivo das regras sobre segurança cibernética da Gestora é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da Gestora devem assegurar:

- a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);

- a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e

- a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da Gestora, observadas as regras de sigilo e confidencialidade constantes do Manual.

Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da Gestora poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

A Hashdex exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

## 2.3 Responsabilidade

### 2.3.1 Responsável pela Segurança Cibernética

O Sr. Samir Kerbage é o(a) responsável por esta Política, sendo o/a principal responsável dentro da Gestora para tratar e responder questões de segurança cibernética ("Responsável pela Segurança Cibernética"), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Segue abaixo uma lista não exaustiva dos deveres e responsabilidades do Responsável pela Segurança Cibernética:

- Testar a eficácia dos controles utilizados e informar ao Comitê de Segurança Cibernética os riscos residuais.

- Acordar com o Comitê de Segurança Cibernética o nível de serviço que será prestado por terceiros contratados e os procedimentos de resposta aos incidentes.

- Configurar os equipamentos e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o número de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Gestora em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros.

- Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da Gestora, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Gestora.

- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Gestora, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente, deverá imediatamente informar o Responsável por Segurança Cibernética, que poderá convocar reunião do Comitê de Segurança Cibernética.

### 2.3.2 Comitê de Segurança Cibernética

O Comitê de Segurança Cibernética será composto pelo: (i) Diretor de *Compliance*, (ii) Responsável pela Segurança Cibernética e (iii) pelo Sr. Bruno Leonardo Kmita de Oliveira Passos, tendo como objetivo a supervisão e monitoramento das regras Segurança Cibernética, conforme aqui previsto.

O Comitê de Segurança Cibernética se reunirá no mínimo trimestralmente/, ou sempre que necessário, mediante convocação por e-mail do Responsável pela Segurança Cibernética, nas reuniões ordinárias, ou de qualquer de seus membros, nos demais casos.

O Comitê de Segurança Cibernética deverá ser instalado necessariamente com a presença do Responsável pela Segurança Cibernética (ou, na sua ausência, seu suplente), a quem caberá a sua coordenação. As deliberações serão tomadas pelo voto da maioria dos presentes, devendo ser lavrada ata das reuniões, a qual deverá ser arquivada no sistema de gerenciamento de *compliance* da Gestora (sistema Compliasset).

### 2.3.3 Demais Atribuições

Caberá a todos os Colaboradores conhecer e adotar as disposições das Políticas de Confidencialidade e Segurança da Informação e da presente Política, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas, o qual recorrerá ao Responsável pela Segurança Cibernética, se for o caso.

Em caso de incidente que afete a segurança cibernética da Gestora, o Colaborador deverá comunicar imediatamente ao Responsável pela Segurança Cibernética, diretamente ou por meio do canal apropriado. Em caso de descumprimento, ainda que involuntário, estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei.

## 2.4 Identificação/Avaliação de riscos (*risk assessment*)

A Gestora periodicamente, no mínimo anualmente, deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção. Esse processo será conduzido pela equipe de TI e a área de gestão da Hashdex, o qual deverá ser documentado pelo Responsável pela Segurança Cibernética com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da Gestora. A Gestora poderá contratar uma empresa terceirizada para tanto, caso o Responsável pela Segurança Cibernética] julgue necessário e mediante aprovação do Comitê de Segurança Cibernética.

Após a condução do referido processo, o Comitê de Segurança Cibernética deverá discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Gestora, considerados os possíveis

impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade do evento acontecer.

Todos os requisitos de segurança da informação e segurança cibernética, incluindo a necessidade de planos de contingência, devem ser previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, na avaliação inicial:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso ("Phishing");
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política;
- Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais ou informações de clientes, como pharming, phishing, vishing e smishing;
- Não conformidade com a política de BYOD; ou
- Vazamento de informações durante tráfego de dados não criptografados.

Periodicamente, no mínimo anualmente, deverá a Gestora revisar o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança de cibersegurança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas corretamente e de forma consistente pelos profissionais designados.

## 2.5 Ações de Prevenção e Proteção

A Gestora estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

**Internet, e-mail e computadores**

A Hashdex oferece a seus Colaboradores uma completa estrutura tecnológica para o exercício das atividades. É de responsabilidade do Colaborador manter e zelar pela integridade dessas ferramentas de trabalho.

Além disso, o Colaborador é responsável pela proteção de seu banco de dados, seja ele composto por planilhas, e-mails e/ou conversas telefônicas contendo dados confidenciais de clientes e/ou da Hashdex, dentre outros.

- Os equipamentos e computadores utilizados pelos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Hashdex e sob nenhuma hipótese servirão de instrumento à discriminação em virtude de raça, religião, cor, origem, idade, sexo, incapacidade física e mental ou de qualquer outra forma não autorizada expressamente em lei;

- A utilização de equipamentos da Hashdex para fins particulares é permitida de forma moderada;

- A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da Hashdex, depende de autorização expressa do Responsável pela Segurança Cibernética e deverá observar os direitos de propriedade intelectual pertinentes, tais como *copyright*, licenças e patentes;

- Os downloads de qualquer natureza devem ser feitos de forma ponderada e com a devida diligência por parte do usuário, respeitando o espaço individual de cada usuário. Periodicamente e sem aviso prévio serão realizadas inspeções nos computadores para averiguação de *downloads* impróprios não autorizados ou gravados em local indevido;

- O correio eletrônico disponibilizado pela Hashdex caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo de utilização preferencial para alcançar os fins comerciais aos quais se destina. É permitida a utilização pessoal de forma moderada;

- As mensagens enviadas ou recebidas através do correio eletrônico corporativo (os "Emails Corporativos"), seus respectivos anexos, e a navegação através da rede mundial de computadores (a "Internet") através de equipamentos da Hashdex poderão ser monitoradas;

- Os E-mails Corporativos recebidos pelos Colaboradores, quando abertos, deverão ter sua adequação às regras desta Política imediatamente verificada. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem;

- Nos equipamentos e computadores disponibilizados pela Hashdex não é recomendado o uso de e-mails públicos (*webmails*) ou qualquer outro tipo de correio eletrônico que não seja o correio corporativo da Hashdex. Fica também proibido a utilização de programas de conversas eletrônicas (CHATs) externos, gratuitos ou não, salvo para fins comerciais, quando autorizado pelo Responsável pela Segurança Cibernética.

**Senhas**

Senhas de caráter sigiloso, pessoal e intransferível serão fornecidas aos Colaboradores para acesso à rede corporativa, sistemas internos e ao correio eletrônico corporativo. Em nenhuma hipótese as senhas deverão ser transmitidas a pessoas que não sejam Colaboradores, sendo os Colaboradores responsáveis pela manutenção de cada senha com suas características.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras passiveis de engenharia social.

**Monitoramento Telefônico**

As conversas telefônicas originadas ou recebidas pelo sistema de telefonia da Hashdex serão monitoradas e gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política, inclusive no âmbito judicial.

**Monitoramento por câmeras**

A Gestora utiliza um serviço de monitoramento por câmeras e são gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política.

### 2.5.1 Procedimentos de Segurança Cibernética de Terceiros

Os Colaboradores externos da Hashdex, dentre os quais os seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de cibersegurança. A computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de Colaboradores externos, envolve determinados riscos que devem ser levados em conta pela Gestora, demandando certos cuidados proporcionais a esta identificação de ameaças.

#### 2.5.1.1 Avaliação dos Terceiros Contratados

A contratação de terceiros se pautará, no que tange à segurança cibernética e conforme se verificará em diligência específica, pelos seguintes critérios:

1. O terceiro deve possuir políticas, programa e procedimentos formais relativos à segurança da informação que sejam auditados e atualizados periodicamente.
2. O terceiro deve possuir plano de resposta a incidentes de segurança cibernética.
3. O terceiro deve realizar, em medida adequada, ações de conscientização, educação e formação de segurança de seus funcionários.

4. O terceiro deve possuir, comprovadamente, mecanismos satisfatórios para proteção dos dados transacionados com a Hashdex.
5. O terceiro deve possuir responsável técnico e deter sistemas e políticas satisfatórias para detecção e reporte de atividades não autorizadas nos sistemas utilizados em sua relação com a Hashdex.
6. O terceiro deve possuir canal de compliance adequado para o reporte completo e tempestivo de incidentes de segurança cibernética, assim como determinar em suas políticas as hipóteses de comunicação de tais incidentes a clientes e/ou reguladores, quando aplicável.
7. O terceiro deve possuir política formalizada de segurança cibernética, e deve manter sempre vigentes e regulares todas as suas certificações necessárias à prestação dos serviços contratados.

Nesse sentido, a área de *Compliance* da Gestora deverá verificar o conteúdo mínimo de *compliance* em segurança cibernética de terceiros que (i) gerem acesso a informações e sistemas confidenciais ou sensíveis, (ii) prestem serviços de computação em nuvem, (iii) tenham conexões lógicas (links) com a Gestora ou (iv) qualquer outros que a área de *Compliance* julgue que por qualquer motivo possa gerar risco de cibersegurança à Gestora, previamente à sua contratação, na forma do Anexo II a esta Política.

O resultado será encaminhado ao Comitê de Segurança Cibernética para avaliação da capacidade deles de evitar ataques cibernéticos e da potencial contratação, devendo a decisão sobre a contratação ficar formalizada, sendo periodicamente reavaliada.

#### 2.5.1.2 Requisitos de Segurança da Informação nos Contratos com Terceiros

A Gestora deverá incluir em contratos com Colaboradores externos requisitos de segurança da informação nos contratos de prestação de serviços, bem como verificar a efetividade dos controles implementados pela empresa contratada para atender aos requisitos durante a vigência do contrato, na forma menciona acima.

### 2.6 Monitoramento e Testes

Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

O ambiente de TI da Gestora será monitorado, por meio de indicadores e geração de histórico, incluindo por exemplo e se aplicável de acordo com a solução adotada: (i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à Internet e aos sistemas críticos da Gestora; (iii) de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Gestora; (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e (v) das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Nessse sentido, a Hashdex investirá continuamente em ferramentas robustas para monitoramento do ambiente, como também na manutenção de equipe especializada com expertise na área

Para garantir as regras mencionadas nesta Política, a Gestora deverá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- Para os riscos associados a pharming, phishing, vishing e smishing, conduzir treinamentos e campanhas periódicas, bem como testes ao menos anualmente;

- Realizar, a qualquer tempo, inspeção física nas máquinas de hardware se mantido servidor físico;

- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e

- Testar a vulnerabilidade e penetração do Website da Gestora, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela Gestora, ao menos semestralmente.

Na realização dos testes e monitoramentos aqui referidos, arquivos pessoais salvos em cada computador ou equipamento da Gestora poderão ser acessados, caso o Comitê de Segurança Cibernética julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

## 2.7 Plano de Resposta a Incidente

A Gestora deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Continuidade de Negócios ("Plano"), considerando os cenários de ameaças lá previstos (que inclui falha de segurança cibernética grave) e os descritos abaixo para os demais casos.

Os Colaboradores poderão reportar incidentes diretamente ao Responsável pela Segurança Cibernética ou por meio do canal de reporte compliance@hashdex.com.

### 2.7.1 Procedimento em Caso de Incidente

Uma vez que o Responsável pela Segurança Cibernética tenha sido acionado devido a um potencial incidente, este deverá convocar o Comitê de Segurança Cibernética para que este delibere sobre a matéria.

**Avaliação Inicial**

Nessa etapa inicial, aspectos e decisões fundamentais deverão analisadas pelo Comitê e tomadas após o incidente. O foco da reunião deverá compreender uma análise do que

aconteceu, motivos e consequências imediatas, bem como a gravidade da situação, devendo decidir pela formalização ou não do incidente.

**Incidente Caracterizado**

Se for caracterizado um incidente, devem os membros do Comitê tomar as medidas imediatas, que poderão abranger se (i) será registrado um boletim de ocorrência ou queixa crime, informar à CVM, ANBIMA ou mais alguma autoridade, (i) é necessário envolver consultor ou advogado externo; (iii) haverá comunicação interna ou externa, em especial a Investidor que tenha sido afetado; e (iv) houve prejuízo para a Gestora, algum veículo de investimento ou investidor específico. Além disso, o Comitê, em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

**Recuperação**

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados. Será realizado um *call* diário ou uma reunião presencial, conforme o caso, em periodicidade a ser definida, para acompanhamento pelo Comitê, com um sumário elaborado pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos.

Também deverá se avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações, tais como manifestação publica na mídia, com eventual contração de PR, enquanto que o Comitê de Investimentos verificará se todas as informações necessárias ao portfólio estão seguras e a área de gestão definirá se decisões de investimento são requeridas. Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados ao Comitê. Colaboradores externos relevantes deverão ser mantidos atualizados.

**Retomada**

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar ao *full compliance*, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A Área de *Compliance* deverá registrar o histórico em local adequado, como o sistema de gerenciamento.

## 2.8 Reciclagem e Revisão

A Gestora deverá manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Também realizará campanha de conscientização em cibersegurança com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger as informações como parte de suas responsabilidades por meio do Programa de Treinamento [previsto na Política de Treinamento] da Gestora.

O Responsável pela Segurança Cibernética, em conjunto com o Comitê de Segurança Cibernética], realizará a revisão e atualização desta Política periodicamente, no mínimo anualmente ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança Cibernética.

## ANEXO I

## TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Através deste instrumento eu, _____, inscrito no CPF/MF sob o nº_____, doravante denominado Colaborador, e Hashdex Gestora de Recursos Ltda.., inscrita no CNPJ/MF sob o n.º 30.056.796/0001-65 ("GESTORA") resolvem, para fim de preservação de informações pessoais e profissionais dos clientes e da GESTORA, celebrar o presente Termo de Responsabilidade e Confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais ("Informações Confidenciais"), para os fins deste Termo:

a) Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e do fundo gerido pela GESTORA, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para o fundo de investimento gerido pela GESTORA, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da GESTORA e a seus sócios ou clientes, independente destas informações estarem contidas em pen-drives, hard-drives, outros tipos de mídia ou em documentos físicos.

b) Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na GESTORA, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da GESTORA e/ou de subsidiárias ou empresas coligadas, afiliadas ou controladas pela GESTORA ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

1.1 Não são consideradas Informações Confidenciais, quaisquer informações que: (i) já forem de domínio público à época em que tiverem sido obtidas pelo Colaborador; (ii) passarem a ser de domínio público, após o conhecimento pelo Colaborador, sem que a divulgação seja efetuada em violação ao disposto neste Termo; (iii) já forem legalmente do conhecimento do Colaborador antes de lhes terem sido reveladas e este não tenha recebido tais informações em confidencialidade; (iv) forem legalmente reveladas ao Colaborador por terceiros que não as tiverem recebido sob a vigência de uma obrigação de confidencialidade; (v) forem ou sejam divulgadas ou requisitadas por determinação judicial, Poder Público e/ou pela autoridade competente, devendo o Colaborador, neste último caso, informar imediatamente ao Diretor de *Compliance* da Gestora para que as medidas legais cabíveis sejam tomadas, observado o disposto no item 5 deste Termo.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na GESTORA, comprometendo-se, portanto, observadas as disposições das Políticas da GESTORA, a não divulgar tais Informações Confidenciais para quaisquer fins ou pessoas estranhas GESTORA, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1 O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na GESTORA.

2.2 As obrigações ora assumidas ainda persistirão no caso do Colaborador ser transferido para qualquer subsidiária ou empresa coligada, afiliada, ou controlada pela GESTORA.

2.3 A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita a apuração de responsabilidades nas esferas cível e criminal.

3 O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a GESTORA e terceiros, ficando desde já o Colaborador obrigado a indenizar a GESTORA, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1 O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho, e desligamento ou exclusão por justa causa do Colaborador se este for sócio da GESTORA, sem prejuízo do direito da GESTORA de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

3.2 O Colaborador expressamente autoriza GESTORA a deduzir de seus rendimentos, sejam eles remuneração, participação nos lucros ou dividendos observados, caso aplicáveis, eventuais limites máximos mensais previstos na legislação em vigor, quaisquer quantias necessárias para indenizar danos por ele dolosamente causados, no ato da não observância da confidencialidade das Informações Confidenciais, nos termos do parágrafo primeiro do artigo 462 da Consolidação das Leis do Trabalho, sem prejuízo do direito da GESTORA de exigir do Colaborador o restante da indenização, porventura não coberta pela dedução ora autorizada.

3.3 A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, mencionados nos itens 2 e 2.1 acima.

3.4 O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

a) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na GESTORA são e permanecerão sendo propriedade exclusiva da GESTORA e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na GESTORA, devendo todos os documentos permanecer em poder e sob a custódia da GESTORA, salvo se em virtude de interesses da GESTORA for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da GESTORA;

b) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à GESTORA todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

c) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da GESTORA, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

d) É expressamente proibida a instalação pelo Colaborador, de softwares não homologados pela GESTORA nos equipamentos utilizados pelo Colaborador para desenvolver suas atividades profissionais.

e) A senha que foi fornecida para acesso à rede de dados institucionais é pessoal e intransferível e não deverá, em nenhuma hipótese, ser revelada a outra pessoa.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a GESTORA, permitindo que a GESTORA procure a medida judicial cabível para atender ou evitar a revelação.

5.1 Caso a GESTORA não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela a que o Colaborador esteja obrigado a divulgar.

5.2 A obrigação de notificar a GESTORA subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a GESTORA, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

6.1 A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas conforme descrito no Código de Ética ou em políticas da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 vias de igual teor e forma, para um só efeito produzirem.

Rio de Janeiro, _____ de _____ de 20___.

_____

COLABORADOR

_____

HASHDEX GESTORA DE RECURSOS LTDA.

## ANEXO II

## MODELO DE DILIGÊNCIA COM TERCEIROS DO GRUPO TÉCNICO DE CIBERSEGURANÇA DA ANBIMA

Conteúdo mínimo de *Compliance* em segurança cibernética a ser verificado

| ***Compliance*** | **Respostas** |
|---|---|
| 1. A empresa tem políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança? a. Se sim, é objeto de teste ou auditoria periódica? b. Se não, está em fase de elaboração? Qual é o prazo de finalização dele para devido envio à instituição contratante? | |
| 2. A empresa apresenta plano de resposta a incidentes de cibersegurança? | |
| 3. A empresa apresenta ações de conscientização, educação e formação de segurança da informação junto a seus funcionários? | |
| 4. Quais são as ferramentas e os mecanismos utilizados para proteção de dados transacionados com a empresa contratante? | |
| 5. Quais são as práticas aplicadas para detectar atividade não autorizadas nos sistemas utilizados? Solicitar também designação de responsável por detectar tais atividades e a quem se reporta. | |
| 6. Na eventualidade de detecção de incidente de cibersegurança, o relato é feito por meio de canais de gestão apropriadas o mais rápido possível? Há comunicação a clientes e/ou reguladores (quando aplicável)? | |
| Favor disponibilizar os seguintes documentos:<br>• Programa de segurança cibernética: se a organização segue políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança, recomenda-se solicitar envio da documentação à empresa contratante para avaliação e arquivamento. Solicitar também o último relatório de teste/auditoria periódica.<br>• Certificações: solicitar envio de certificações que possam comprovar a devida capacidade técnica do prestador de serviço. | |