POLÍTICA DE SEGURANÇA CIBERNÉTICA

ATUALIZAÇÃO: JUNHO 2020

Versão: 1.2
Diretoria responsável: Compliance & Riscos
Escopo: Colaboradores HIX Capital

ÍNDICE GERAL

Sumário

Introdução

A Política de Segurança Cibernética ("Política") tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética da HIX Investimentos Ltda. ("HIX Investimentos" ou "Gestora"), no intuito de minimizar as ameaças a sua imagem e aos seus negócios.

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

1. Princípios da Segurança dos dados e dos sistemas de informação

O objetivo das regras sobre segurança cibernética da Gestora é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança 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 da Política de Confidencialidade constante no Código de Ética e Manual de Compliance Gestora.

Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional contratada pela HIX Investimentos pertence à Gestora. 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 HIX Investimentos 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. Responsabilidade

2.1. Responsável pela Segurança Cibernética

O Francisco Dergham Ajaj é o responsável por esta Política, sendo o 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.

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

- Testar a eficácia dos controles utilizados e informar aos Diretores executivos da HIX Investimentos os riscos residuais.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política, bem como definir e assegurar a segregação das funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo, eliminando, ou ao menos reduzindo, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, mantendo evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Gestora.
- Planejar, implantar, fornecer, e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Proteger continuamente todos os ativos de informação da Gestora contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- 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.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da Gestora operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Gestora.
- Garantir um backup em nuvem, devidamente criptografado.
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Gestora, mediante campanhas, treinamentos e outros meios de endomarketing.

3. Identificação e Avaliação de Riscos (risk assessment)

A Gestora, em periodicidade mínima anual, identifica e avalia os riscos cibernéticos 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 pelo Responsável pela Segurança Cibernética da HIX Investimentos, 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 e seus riscos de segurança cibernética. A Gestora poderá contratar uma empresa terceirizada para tanto, caso o Responsável pela Segurança Cibernética julgue necessário e mediante aprovação dos Diretores Executivos da HIX Investimentos

Após a condução do referido processo, o Diretor de Compliance deverá discutir as opções de tratamento a serem adotadas com os Diretores Executivos, 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.

A HIX Investimentos entende que os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

3.1. Ataques cibernéticos

Os ataques cibernéticos mais comuns são:

- Malware – softwares desenvolvidos para corromper os computadores e redes, como:
  - Vírus: software que causa danos à máquina, rede, softwares e Banco de Dados;
  - Cavalo de Troia: aparece dentro de outro software criando uma porta para a invasão do computador;
  - Spyware: software malicioso para coletar e monitorar o uso de informações; e
  - Ransomware: software malicioso que bloqueia o acesso aos sistemas e base de dados, solicitando um resgate para que o acesso seja reestabelecido.
- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como exemplo:
  - Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
  - Phishing: links vinculados por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
  - Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
  - Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
- Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes, a fim de captar qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição.
- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a HIX Investimentos pode estar sujeita a má funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

3.2. Ações de prevenção e proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para HIX Investimentos, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Gestora, em caso de incidente de segurança.

Deste modo, a Gestora segrega as informações geradas pela instituição, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classificam-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

- Green Flag:
  - Quaisquer informações e/ou dados que a HIX Investimentos teve acesso ou conhecimento por ser de domínio público (“Informação Pública”);
  - Quaisquer informações e/ou dados que não estejam sujeitos a compromissos ou acordos de confidencialidade; ou
  - Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

- Yellow Flag:
  - Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

- Red Flag:
  - Todas as Informações Confidenciais, a saber:
  - Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela HIX Investimentos;
  - Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Gestora; e

- 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/ou de seus sócios e clientes.
- Todas as informações de Terceiros que sejam consideradas Informações Confidencias ou Informações Sensíveis, conforme disposto no Código de Ética.

A Gestora estabeleceu um conjunto de medidas buscando mitigar os riscos identificados conforme seu grau de criticidadade consoante acima definido, ou seja, a HIX Investimentos busca impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, dispostos ao longo deste Política. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

A partir desse ponto, passamos a mencionar os procedimentos de prevenção e proteção adotados pela Gestora:

3.3. Estrutura de TI

A HIX Investimentos cataloga os seus principais equipamentos, procedimentos e sistemas de Tecnologia da Informação, qual segue lista exemplificativa abaixo:

- Backup diário local e externo;
- 1 (Um) link de Internet Dedicado da Algar;
- 1 (Um) link de Internet Empresaria da VIVO;
- Duas impressoras;
- 1 (Uma) Central PABX IP da Algar com 25 ramais;
- Linhas de telefone digitais;
- Aparelhos de telefone IP;
- Computadores corporativos DELL Optiplex com acesso à Intranet/Internet, todos com extensão de garantia de hardware;
- Acesso ao sistema de informações de posição dos fundos e gerenciamento de riscos fornecido pela Investtols, e ao sistema de gestão de ordens e gerenciamento de Compliance Pré e pós trading, fornecido pela EZE Software;
- Sistema de Firewall redundante com sistema de detecção de intrusos e bloqueio automático com acesso auditados da marca Sophos;
- Switches Giga e a rede local (Giga Ethernet);
- Sistema de correio eletrônico com anti-spam e recursos de regras para controle de envio de e-mails fornecido pela Microsoft Office 365;
- Grupo gerador no condomínio com gerenciamento e tanque com autonomia média de 4 horas ininterruptas, sem reabastecimento, garantindo energia para o escritório em São Paulo;
- Nobreak com gerenciamento, para prevenção de surtos elétricos e estabilização elétrica de todas as tomadas dos equipamentos sensíveis da empresa, como os ativos de TI e mesa de operação;
- CPD local climatizado com acesso restrito ao local;
- Sistema de Proxy com regras de conteúdo de acesso às páginas da internet;

3.3.1. Propriedade dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da HIX Investimentos. Não é permitida a utilização de notebooks, tablets ou outros hardwares pessoais para operações no âmbito da Gestora, salvo expressa permissão do Diretor de Compliance.

3.3.2. Disponibilização e Uso

A utilização dos ativos da HIX Investimentos, incluindo computadores, telefones, Internet, programas de mensagem instantânea, e-mails e demais aparelhos se destina exclusivamente a fins profissionais, e deve ser feita com cuidado.

Todo o processo de criação e exclusão de usuário, instalação de softwares e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela área responsável, mediante aprovação do Responsável pela Segurança Cibernética.

A disponibilização e uso dos computadores da HIX Investimentos respeitam as seguintes regras:

- A cada novo Colaborador, o Diretor de Compliance autoriza, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão e aprovação do Responsável pela Segurança Cibernética;
- O Responsável pela Segurança Cibernética autoriza, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área responsável, mediante supervisão e aprovação do Responsável pela Segurança Cibernética;
- A identificação do usuário é feita através do login e senha, que através do registro de logs utilizado pela HIX Investimentos é sua assinatura eletrônica no servidor da Gestora;
- São apenas permitidas senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 03 (três) vezes;
- Não é recomendado a utilização da mesma senha para projetos e serviços diferentes realizados pela HIX Investimentos, evitando criar uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue;
- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da expiração da mesma;
- Todos os eventos de login e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de Compliance à área responsável;
- Todo e qualquer e-mail ou mensagem instantânea (“MI”) que constitua um livro ou registro sobre qualquer atividade, transação ou negócio da Gestora será mantido pela HIX Investimentos;
- É proibida a conexão de qualquer equipamento na rede da HIX Investimentos sem a prévia autorização pelas áreas de informática e do Responsável da Segurança Cibernética; e

- A Gestora implementou controles robustos de acesso utilizando duplo fator de autenticação em seu sistema de e-mail e nos sistemas críticos da HIX Investimentos (Controle de acesso lógico adequado aos ativos da organização).

A Gestora reconhece que, em determinados casos, a MI pode ser uma fonte valiosa de informação, bem como um método eficiente de comunicação. A Gestora, portanto, permite aos Colaboradores usar o recurso de MI para comunicações relacionadas a suas atividades. Os Colaboradores são os responsáveis por todo o conteúdo trafegado por MIs, e caso seja comprovado que essa ferramenta foi utilizada de forma indevida, o colaborador será penalizado de acordo com decisão do Comitê de Compliance.

3.3.3. Two-factor Authentication

Os equipamentos móveis utilizados na gestora são pessoais de cada um. Os colaboradores deverão aceitar o acesso da Tecnoqualify para configurar o e-mail coorporativo, bem como seguir as regras de segurança estabelecidas (instalação do Two-factor authentication - 2FA). Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a equipe de TI mediante registro de chamado junto ao Responsável pela Segurança Cibernética. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário. Documentos imprescindíveis para as atividades dos Colaboradores da Gestora deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

Todos os computadores de uso individual serão ingressados no domínio HIXCAPITAL de modo que para o acesso a máquina cada usuário deverá utilizar sua credencial. Os usuários não são administradores das máquinas, não tendo privilégios para acessar conteúdo no perfil de outro possível usuário logado.

Os Colaboradores devem informar ao Responsável pela Segurança Cibernética, por meio formal, qualquer identificação de dispositivo estranho conectado ao seu computador.

É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da equipe de TI ou por terceiros devidamente contratados para o serviço.

Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização do Responsável pela Segurança Cibernética.

Todas as contas deverão ter o Two-factor authentication - 2FA devidamente ativado.

3.3.4. Dispositivos Móveis

Considerando que deseja facilitar a mobilidade e o fluxo de informação entre seus Colaboradores, a HIX Investimentos permite o uso de seus equipamentos portáteis. Por "dispositivo móvel", entende-se qualquer equipamento eletrônico com atribuições de mobilidade como: notebooks, smartphones e tablets.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os Colaboradores que utilizem tais equipamentos.
O Colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na HIX Investimentos, mesmo depois de terminado o vínculo contratual mantido com a Gestora.

Todo Colaborador deverá ter o Two-factor authentication (2FA) devidamente instalado na sua conta de e-mail, configurado nos dispositivos móveis.

É permitido o uso de rede banda larga de locais conhecidos pelo Colaborador como: sua casa, hotéis, fornecedores e clientes. O Colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará que assumiu todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à Gestora e/ou a terceiros.

3.3.5. Datacenter

O acesso ao Datacenter somente deverá ser feito por pessoas autorizadas como os diretores executivos, responsável pela Segurança Cibernética e pela Tecnoqualify.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um Colaborador autorizado.

A chave da porta do Datacenter deverá ficar na posse do Responsável pela Segurança Cibernética, ou Colaborador definido por este.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a autorização do Responsável pela Segurança Cibernética.

3.3.6. Uso de e-mail

É proibido a utilização profissional de correio eletrônico particular.

A HIX Investimentos disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@hixcapital.com.br)

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Gestora.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a HIX Investimentos.

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Compliance.

O usuário pode acessar o seu correio eletrônico cedido pela HIX Investimentos mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da Gestora.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da HIX Investimentos, inclusive que contenha fins políticos locais ou do país (propaganda política). O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente.

Acrescentamos que é proibido aos Colaboradores o uso de e-mail da HIX Investimentos para as seguintes atividades:

- Sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da HIX Investimentos;
- Sejam incoerentes com o Código de Ética Corporativa da Gestora;
- Enviar mensagens (i) não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Gestora; (ii) pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar; (iii) que torne seu remetente e/ou a Gestora vulnerável a ações civis ou criminais; (iv) que inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a Gestora estiver sujeita a algum tipo de investigação; e
- Produzir, transmitir ou divulgar mensagem que (i) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Gestora; (ii) contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador; (iii) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança, bem como que vise:
    - obter acesso não autorizado a outro computador, servidor ou rede;

- interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- burlar qualquer sistema de segurança;
- vigiar secretamente ou assediar outro usuário;
- acessar informações confidenciais sem explícita autorização do proprietário;
- acessar indevidamente informações que possam causar prejuízos a qualquer pessoa; e
- inclua imagens criptografadas ou de qualquer forma mascaradas;

As mensagens de e-mail deverão incluir assinatura com o seguinte formato: (i) nome do Colaborador, Nome da empresa, Disclaimer, Telefone(s) e Correio eletrônico.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da HIX Investimentos é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da Gestora.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
- Ao uso da opção encaminhar (Forward), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

3.3.7. Uso da internet

Todas as regras atuais da HIX Investimentos visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da Internet. Embora a conexão direta e permanente da rede corporativa com a Internet ofereça um grande potencial de benefícios, também propicia riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na Internet está sujeita a divulgação e auditoria. Portanto, a Gestora reserva-se o direito de monitorar e registrar todos os acessos a ela, nos termos da legislação aplicável. Como mencionado, os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet são de propriedade da Gestora, que pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede/Internet, estejam em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

A visualização de sites, blogs, fotologs e webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física) obsceno, pornográfico ou ofensivo é terminantemente proibida.

Programas licenciados e instalados nos computadores, principalmente via Internet ("downloads"), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do Responsável pela Segurança Cibernética.

Qualquer software não autorizado baixado poderá excluído pela equipe de TI. Os Colaboradores não poderão em hipótese alguma utilizar os recursos da Gestora para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à HIX Investimentos ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados. Os Colaboradores não poderão utilizar os recursos da Gestora para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos, conforme definido pelo Diretor de Compliance.

O usuário também está proibido de a acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes;
- Contenham informações que não colaborem para o alcance dos objetivos da HIX Investimentos;
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo superior. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Gestora cooperará ativamente com as autoridades competentes.

Periodicamente, a Área de Compliance e o Responsável pela Segurança Cibernética revisarão e bloquearão o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Gestora.

3.3.8. Identificação e uso de senhas

Observado o disposto na Política de Confidencialidade e Segurança da Informação, a senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails, que também devem ser

acessados via webmail, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

Todos os dispositivos de identificação utilizados na HIX Investimentos, como o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a Gestora e a legislação (cível e criminal).

É também proibido o compartilhamento de login para funções de administração de sistemas. A área administrativa da HIX Investimentos é a responsável pelo controle dos documentos físicos de identidade dos Colaboradores.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários não possuem perfil de administrador. E as senhas deverão ter pelo menos 8 caracteres, sendo um deles, especial, e são renovadas a cada 180 dias, sendo que as 3 últimas não poderão ser repetidas obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

A periodicidade máxima para troca das senhas é 180 dias, não podendo ser repetida a última senha. Os sistemas críticos e sensíveis para a Gestora e os logins com privilégios administrativos devem exigir a troca de senhas a cada 180. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, a Área Administrativa deverá imediatamente comunicar tal fato à equipe de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

3.3.9. Reprodução e Descarte

É terminantemente proibido aos Colaboradores fazer cópias ou imprimir arquivos usados, gerados ou disponíveis na rede da HIX Investimentos e circular em ambientes externos a HIX Investimentos com esses arquivos, uma vez que tais arquivos contêm informações consideradas confidenciais.

A proibição acima não se aplica quando as cópias ou impressão de arquivos forem usadas para executar ou desenvolver negócios e interesses da HIX Investimentos. Nestes casos, os Colaboradores em posse e

guarda da cópia ou do arquivo impresso contendo as informações confidenciais serão diretamente responsáveis por sua boa conservação, integridade e manutenção de sua confidencialidade.

O descarte de informações confidenciais em meio digital ou físico deve ser feito de forma a impossibilitar sua recuperação.

Em consonância com as normas acima, os Colaboradores devem abster-se de utilizar pen drives, disquetes, fitas, discos ou quaisquer outras mídias que não exclusivamente para o desempenho de sua atividade na HIX Investimentos.

Todas as informações que possibilitem a identificação de um Investidor da HIX Investimentos devem permanecer em arquivos de acesso restrito, e somente poderão ser copiadas ou impressas para o atendimento dos interesses da HIX Investimentos ou do próprio Investidor. Tal restrição não se aplica na eventualidade de cumprimento de ordem de autoridade judicial ou extrajudicial determinando a disponibilização de informações sobre eventual Investidor da HIX Investimentos, cujo atendimento deverá ser previamente comunicado ao Diretor de Compliance.

3.3.10. Armazenamento em Nuvem (Cloud)

A HIX Investimentos poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (Cloud).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

Almejando mitigar eventuais incidentes cibernéticos, a Gestora, quando realizar o Armazenamento de dados na Nuvem, contará com um sistema de Antivírus e com Firewall.

3.4. Procedimentos de Segurança Cibernética de Terceiros Contratados

Os Colaboradores externos da HIX Investimentos, dentre os quais os seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de segurança cibernética. 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.

Nesse sentido, o Responsável pela Segurança Cibernética 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.

A análise do conteúdo descrito no parágrafo acima será feita por meio de(o) (i) documentos que atestem a existência dos respectivos procedimentos de segurança cibernética; (ii) último relatório de

teste/auditoria periódica; (iii) certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

O resultado deverá avaliar a capacidade deles de evitar ataques cibernéticos e da potencial contratação, devendo a decisão sobre a contratação ficar formalizada, sendo periodicamente reavaliada.

Somente após a aprovação pelo Comitê de Compliance e pelo Responsável pela Segurança Cibernética, o Terceiro poderá ser contratado para prestar serviços de Armazenamento na Nuvem.

Em caso de qualquer incidente constatado pelo Terceiro, este deverá de imediato enviar uma notificação relatando o ocorrido à HIX Investimentos, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.

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.

4. Monitoramento e Testes periódicos

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

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 Risco e Compliance julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Gestora esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da HIX Investimentos.

Ademais, serão realizados Testes Periódicos de Segurança Cibernética da HIX Investimentos, com especial enfoque em segregação lógica, testes de penetração, resposta a eventos de vazamento de dados, rastreabilidade dos logs de acessos às informações sensíveis, tratamento de dados, dentre outros, sempre objetivando a preservação dos dados mantidos pela Gestora, em especial os confidenciais. Referidos testes serão realizados, com periodicidade mínima semestral, pela empresa de TI terceirizada e o resultado será consolidado no relatório anual de controles internos da HIX Investimentos.

5. Plano de Resposta a Incidentes

A Gestora deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Continuidade de Negócios, 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.

5.1. Procedimento em caso de incidente

Uma vez que o Responsável pela Segurança Cibernética tenha sido acionado devido a um potencial incidente, este deverá se reunir com o TI e convocar o Comitê de Risco e Compliance.

5.1.1. Avaliação Inicial

Nessa etapa inicial, aspectos e decisões fundamentais deverão ser analisadas pelo Comitê de Risco e Compliance 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.

5.1.2. Incidente Caracterizado

Se caracterizado o incidente, a HIX Investimentos deverá em conjunto com a empresa de TI terceirizada tomar as seguintes providências:

- Verificação e Auditoria dos Logs;
- Criação de laudo pericial contendo as informações que foram potencialmente vazadas;
- Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;
- Desinstalação de software;
- Execução de varreduras offline para descobrir quaisquer ameaças adicionais;
- Formatação e reconstrução do sistema operacional;
- Substituição física de dispositivos de armazenamento
- Reconstrução de sistemas e redes;
- Restauração de dados provenientes do Backup realizado diariamente;
- Entre outros.

Sem prejuízo, os membros do Comitê de Risco e Compliance devem 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 referido Comitê, em conjunto com eventual consultor, deverá definir os passos a serem tomados sob o aspecto de segurança cibernética, 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.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Após a realização da auditoria sobre o incidentes e seus impactos, a HIX Investimentos deverá, independentemente da contratação de escritório de advocacia externo ou de serviços de TI, proceder com:

- A criação de relatório baseado no laudo pericial elaborado pela Empresa de TI Terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança;
- A elaboração de notificação aos clientes afetados informando o ocorrido, caso haja a confirmação do incidente de segurança e eventual vazamento de informações confidenciais.
- A análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Companhia;
- Realizar planejamento de contenção de risco de liquidez frente à possibilidade de resgate de investimentos da HIX Investimentos resultantes do incidente de segurança.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados pela Área de Compliance, bem como devem ser formalizados no Relatório de Controles Internos da HIX Investimentos.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética e do Manual de Compliance da Gestora.

5.1.3. 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 acompanhamento, conforme o caso, em periodicidade a ser definida, 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 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 Responsável pela Segurança Cibernética.

5.1.4. 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.

6. Treinamento, Reciclagem e Revisão

A HIX Investimentos possui um processo de integração e treinamento inicial e um programa de reciclagem contínua dos conhecimentos de seus Colaboradores com relação aos princípios gerais e normas de Compliance da Gestora, bem como às principais Leis e normas aplicáveis às suas atividades, conforme preceitua a Instrução CVM nº 558/15.

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 segurança cibernética, 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 da Gestora, disposta no Manual de Compliance da HIX Investimentos.

6.1. Demais atribuições

Caberá a todos os Colaboradores conhecer e adotar as definições da Política de Confidencialidade contida no Código de Ética, bem como 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 relacionadas à segurança cibernética, o qual recorrerá ao Responsável pela Segurança Cibernética, se for o caso.

Em caso de incidente que afete a segurança cibernética da Gestora e/ou descumprimento desta Política ou da Política de Confidencialidade, 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.

7. Vigência e Atualização

O Responsável pela 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 Responsável pela Segurança Cibernética.

Termo de Conhecimento da Política de
SEGURANÇA CIBERNÉTICA

NOME
ÁREA
CARGO
DOC. IDENTIDADE Nº
TIPO CPF

Declaro que tenho conhecimento da Política de SEGURANÇA CIBERNÉTICA e que estou ciente do seu teor, o qual está diretamente ligado ao exercício de minhas funções.

De acordo com este termo, comprometo-me a:

a) Adotar e cumprir as diretrizes indicadas na política;

b) Comunicar imediatamente responsável por Compliance qualquer violação dessa política que venha a tornar-se do meu conhecimento, independente de qualquer juízo individual, materialidade ou relevância da violação. Estou ciente de que meus acessos físicos, lógicos, de voz e de imagem podem ser objeto de monitoramento.

Desde já, aceito incondicionalmente, sempre que solicitado, atender e cumprir quaisquer novos itens e condições que possam vir a ser considerados partes integrantes desta Política, sem a necessidade de apor assinatura em novo termo, bem como em caso de negligência ou imprudência na aplicação desta Política, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

_____, _____ de _____ de 20_____

_____
Assinatura do Colaborador