POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

1. Introdução

A Política de Segurança das Informações e de Segurança Cibernética da Helix Consultoria de Valores Mobiliários - **"Consultoria")** formaliza o seu compromisso com a proteção de Informações Sigilosas e Segurança Cibernética (*cybersecurity*), conforme definição adiante, devendo ser cumprida por todos os Colaboradores.

Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança de Informações Sigilosas. Responsável: Diretor de Gestão de Riscos.

2. Objetivo

Esta Política visa proteger as Informações Sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e audibilidade das mesmas, conforme art. 4º, §8º, da Resolução CVM n.º 021/2021, bem como aprimorar a segurança cibernética da Gestora, nos termos do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, seguindo as recomendações e diretrizes do Guia de Cibersegurança da ANBIMA.

Como regra geral, nenhuma Informação Sigilosa deve ser divulgada, dentro ou fora da Consultoria, a pessoas que não tenham necessidade ou autorização para acessá-la no desempenho de suas atividades profissionais. Qualquer informação, independentemente de ser classificada como Informação Sigilosa – seja relacionada à Consultoria, suas atividades, sócios, fundos, clientes ou obtida no exercício das atividades normais do Colaborador – só poderá ser divulgada ao público, à mídia ou a terceiros de qualquer natureza conforme previsto nos documentos internos da Consultoria.

Na falta de previsão expressa, a revelação ou fornecimento somente poderá ocorrer com o conhecimento e, dependendo do caso, autorização prévia do Diretor de Gestão de Riscos.

3. Aplicação

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Sigilosas e dos Ativos disponibilizados pela Consultoria ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela Consultoria, sendo de responsabilidade individual e coletiva o seu cumprimento.

4. Responsabilidades na Gestão da Política

Cabe a todos os Colaboradores:

a) Cumprir fielmente esta Política;
b) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das Informações Sigilosas;
c) Proteger Informações Sigilosas contra acesso, modificação, destruição ou divulgação não autorizados pela Consultoria;
d) Assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela Consultoria;
e) Cumprir as leis e normas que regulamentam os aspectos relacionados ao direito autoral e propriedade intelectual no que se refere às Informações Sigilosas;

f) Comunicar imediatamente a Área de Gestão de Riscos sobre qualquer descumprimento ou violação desta Política.

5. Conceitos e Princípios

Todas as Informações Sigilosas constituem ativos de valor para a Consultoria, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Consultoria, Clientes, Fundos e Colaboradores.

As Informações Sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança de Informações Sigilosas deve ser prioridade constante da Consultoria, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos da Consultoria. Assim, por princípio, a guarda e segurança das Informações Sigilosas deve abranger três aspectos básicos, destacados a seguir:

a) Acesso: Somente pessoas devidamente autorizadas pela Consultoria devem ter acesso às Informações Sigilosas;
b) Integridade: Somente alterações, supressões e adições autorizadas pela Consultoria devem ser realizadas às Informações Sigilosas;
c) Disponibilidade: As Informações Sigilosas devem estar disponíveis para os Colaboradores autorizados sempre que necessário ou for demandado.

Para assegurar os 3 (três) aspectos acima, as Informações Sigilosas devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

Em cumprimento ao Guia Anbima de Segurança Cibernética, a Consultoria possui cinco pilares principais no seu programa de segurança cibernética:

a) Identificação e avaliação de riscos (*risk assessment*);
b) Ações de prevenção e proteção;
c) Monitoramento e testes;
d) Plano de resposta.

A implantação e monitoramento da capacidade da Consultoria atender a estes pilares deverá ser feito pelo Diretor de Gestão de Riscos. Também a fim de atingir os objetivos dispostos acima, cada segmento de atuação da Consultoria terá suas próprias responsabilidades.

A Consultoria deverá ter uma abordagem holística em relação à segurança cibernética, sendo obrigação do Diretor de Gestão de Riscos promover treinamentos para que os Colaboradores saibam as suas respectivas funções na proteção de Informações Sigilosas, para que possam agir de maneira apropriada frente as situações que requeiram respostas.

6. Modelo Adotado

A Consultoria optou por não manter time próprio dedicado à segurança das informações, segurança cibernética, contingência e outros assuntos relacionados com tecnologia da informação, inclusive para a realização de tarefas (instalações, substituições, configurações), verificações e manutenções periódicas.

Dessa mesma maneira, a Consultoria não mantém grupos de trabalho ou outros fóruns para tratar de segurança cibernética. Quando necessário, as matérias a esta relacionadas serão apresentadas pelo Diretor de Gestão de Riscos e tratadas no Comitê de Gestão de Riscos.

7. Procedimentos de Segurança Cibernética

7.1. Identificação e Avaliação de Riscos (*Risk Assessment*)

A Consultoria deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Código Anbima de Segurança Cibernética definiu que os ataques mais comuns de criminosos cibernéticos (*cybercriminals*) são os seguintes:

a) *Malware* (vírus, cavalo de troia, *spyware* e *ransomware*);
b) Engenharia Social;
c) *Pharming*;
d) *Phishing scam;*
e) *Vishing;*
f) *Smishing;*
g) *Acesso pessoal;*
h) *Ataques de DDoS e botnets;*
i) *Invasões* (*advanced persistent threats*).

7.2. Ações de Prevenção e Proteção

A Consultoria adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso à sede e à rede, incluindo aos servidores. A Consultoria trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados.

Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a Consultoria deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A Consultoria conta com recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* pessoais. Da mesma maneira monitora o acesso a websites e restringe a execução de *softwares* e/ou aplicações não autorizadas.

A Consultoria realiza, também, *backup* das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do Plano de Continuidade do Negócio.

7.3. Monitoramento e Testes

Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na Consultoria ou por esta disponibilizados para serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente da Consultoria, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (*software* e/ou *hardware*), pela Área de Gestão de Riscos e/ou por prestador de serviços externo.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da Consultoria, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

A Consultoria possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de *hardware* e *software* atualizados, bem como os sistemas operacionais e *softwares* de uso atualizados.

Periodicamente, a Consultoria realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, em linha, inclusive, com o Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da Consultoria. Dentre as medidas, incluem-se, mas sem se limitar:

a) Verificação dos logs dos Colaboradores;
b) Alteração periódica de senha de acesso dos Colaboradores;
c) Segregação de acessos;
d) Manutenção trimestral de todo os hardwares;
e) Backup diário, realizado na nuvem.

Sem prejuízo dos testes realizados na forma do Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da Consultoria, a Consultoria realizará simulações de ataques e respostas da Consultoria que seriam possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da Consultoria, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

O backup de todas as informações armazenadas nos servidores será realizado na forma descrita no Plano de Contingência e Continuidade de Negócios da Consultoria, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

As rotinas de *backup* são periodicamente monitoradas.

7.4. Plano de Resposta

Havendo indícios ou de suspeita fundamentada, a empresa contratada deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento.

Na hipótese de vazamento de Informações Sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado.

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

Eventos que envolvam a segurança das Informações Sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão formalizados em relatório para deliberação durante o Comitê de Gestão de Riscos. Tanto o evento, quanto as medidas corretivas adotadas e a deliberação do comitê deverão, ainda que sumariamente, constar no Relatório de Controles Internos.

8. Diretrizes de Segurança da Informação

8.1. Adoção de Comportamento Seguro

Independentemente do meio e/ou da forma em que se encontrem, as Informações Sigilosas podem ser encontradas na sede da Consultoria e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

a) Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;
b) Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das Informações Sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;
c) Todo tipo de acesso aos dados e informações da Consultoria, em especial as Informações Sigilosas, que não for expressamente autorizado é proibido;
d) Assuntos relacionados ao desempenho de atividades e funções na Consultoria não devem ser discutidos em ambientes públicos ou em áreas expostas (meios de transporte, locais públicos, encontros sociais);
e) As senhas de acesso do Colaborador aos sistemas da Consultoria são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores), anotadas em papel ou em sistema visível ou de acesso não protegido;
f) Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;
g) Somente softwares homologados e previamente aprovados pela Consultoria podem ser instalados e usados nas estações de trabalho, o que deve ser feito com exclusividade pela equipe de serviços de informática da Consultoria;
h) Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da Consultoria;
i) Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter Informações Sigilosas. Portanto, não podem ser parciais ou totalmente divulgadas, usadas ou reproduzidas sem o consentimento prévio do remetente ou do autor. Toda e qualquer divulgação, uso e/ou reprodução não expressamente autorizada é proibida;

j) O acesso remoto à rede, às Informações Sigilosas e sistemas da Consultoria somente será permitida mediante autorização do Diretor de Gestão de Riscos, e desde que seja estritamente necessário para o desempenho das

funções do Colaborador. O Colaborador será corresponsável pela segurança do acesso remoto aos sistemas e Informações Sigilosas da Consultoria;

k) O Colaborador deve evitar realizar acesso remoto à rede da Consultoria a partir de um dispositivo público, e, caso o faça, deverá limpar o cache e deletar todos os arquivos temporários;
l) Documentos impressos e arquivos contendo Informações Sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da Consultoria sem a autorização prévia do superior hierárquico do Colaborador.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Consultoria. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento à terceiros, bem como com conteúdo político ou outro que possa colocar a Consultoria em risco.

A Consultoria se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus Colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da Consultoria e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

A Área de Gestão de Riscos implantará as medidas necessárias para realizar o monitoramento, bem como para a estabelecer as permissões de acesso aos documentos e arquivos da Consultoria. Nesse sentido, o monitoramento poderá ser realizado pela Área de Gestão de Riscos mediante:

a) Gravação dos ramais telefônicos internos;
b) Gravação em vídeo do ambiente da sede da Consultoria;
c) Registro de mensagens de e-mail;
d) Registro de acesso à Internet;
e) Registro de acesso à rede interna;
f) Registro de acesso à documentos e arquivos;
g) Outros tipos de gravação e registro implantados pela Consultoria.

Esse monitoramento poderá ser realizado automaticamente (*software* e/ou *hardware*), pela Área de Gestão de Riscos e/ou por prestador de serviços externo. Apenas a Área de Gestão de Riscos poderá acessar os arquivos contendo as gravações e registros do monitoramento realizado, bem como, mediante autorização prévia do Diretor Responsável. O Diretor de Gestão de Riscos poderá contratar prestadores de serviços externos para realizar o monitoramento.

O acesso será realizado aleatoriamente, de maneira inopinada e sem periodicidade definida. Os documentos, dados e informações encaminhados pelos prestadores de serviços serão para uso exclusivo do Diretor de Gestão de Riscos.

Sempre que necessário será lavrado termo de monitoramento e acesso aos arquivos contendo registros e gravações.

8.2. Gestão de Acesso a Sistemas de Informação e a Outros Ambientes Lógicos

O uso das Informações Sigilosas e dos recursos de tecnologia disponibilizados pela Consultoria são monitorados, e os registros decorrentes do uso poderão ser utilizados para verificação e evidência da adequação das regras desta Política, e demais regras internas da Consultoria, através de monitoramento a ser efetuado pela Área de Gestão de Riscos.

Todo acesso às Informações Sigilosas, aos ambientes lógicos e à sede da Consultoria deve ser controlado, de forma a garantir acesso apenas às pessoas expressamente autorizadas pela Área de Gestão de Riscos.

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

a) Pedido formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas;
b) Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações e omissões;
c) Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a Política de Segregação das Atividades;
d) Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da Consultoria, ou que tenham mudado de função, se for o caso;
e) Revisão periódica das autorizações concedidas.

8.3. Utilização da Internet

O uso da Internet deve restringir-se às atividades relacionadas aos negócios e serviços da Consultoria, e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

8.4. Websites na Internet

O acesso à sites externos na Internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da Consultoria.

Adicionalmente, a Área de Gestão de Riscos poderá ser informada sobre acessos e tentativas de acesso à determinados sites.

8.5. Ramais Telefônicos

Os ramais telefônicos utilizados na sede da Consultoria pelos Colaboradores da Área de Gestão e da Área Comercial são gravados, e o conteúdo das conversas são armazenados em arquivos nos servidores da Consultoria. Conforme já esclarecido anteriormente, a Área de Gestão de Riscos possui livre acesso as gravações com o propósito de verificação de conteúdo.

Ao término da verificação, a Área de Gestão de Riscos emitirá termo de monitoramento, nos termos do Anexo I, informando o arquivo acessado, a data do acesso e se foram identificados indícios que possam indicar eventual infração ao disposto nesta Política, e nos demais documentos internos da Consultoria.

8.6. Telefones Celulares

Os Colaboradores deverão evitar utilizar telefones celulares durante o horário de expediente enquanto estiverem na sede da Consultoria. Os aparelhos deverão ser mantidos no modo “silencioso” e somente poderão ser atendidas ligações pessoais de reconhecida importância Consultoria.

8.7. Mensagens Instantâneas

A comunicação por mensagens instantâneas de texto e voz pela Internet para assuntos particulares deve ser evitada durante o horário de expediente, enquanto os Colaboradores estiverem na sede da Consultoria, mas não

está proibida. Em caso de necessidade, os Colaboradores devem permitir o acesso a todas as mensagens instantâneas com o propósito de avaliar eventuais infrações ao disposto nos documentos internos.

8.8. Utilização e Conexão de Equipamentos

Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Consultoria.
A utilização de equipamentos pessoais por terceiros nas instalações da Consultoria e a conexão destes na rede interna e à Internet requer autorização prévia e expressa da Área de Gestão de Riscos. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.

A conexão de dispositivos móveis de armazenamento (USB Drive) somente poderá ser realizada mediante autorização prévia e expressa da Área de Gestão de Riscos.

8.9. Acesso de Terceiros

O acesso de terceiros aos arquivos e sistemas da Consultoria será possível, na forma definida pelo Diretor de Gestão de Riscos, mas deve sempre ser precedido da assinatura de um contrato de confidencialidade que estabeleça penalidade no caso de infração. Ademais, o terceiro deverá garantir à Consultoria, ainda que contratualmente, de que possui os controles necessários à boa guarda e proteção das informações aos quais terá acesso.

9. Endereço Eletrônico

Eventuais comunicações para a Área de Gestão de Riscos devem ser enviadas para: Luciana.piai@helixconsult.com.br

10. Recursos computacionais

A Consultoria utiliza um conjunto de softwares na nuvem para desempenho de suas atividades, quais sejam:
Google Drive

- Com relação aos recursos computacionais a Consultoria contará com:
- 3 notebooks, modelo IdeaPad 3i, com Processador Intel® Core™ i3-10110U (4MB Cache, 2.10 GHz), 4GB memória RAM, Placa de vídeo Intel UHD Graphics e HD 128 GB SSD M.2 2242 NVMe
- 1 Impressora samsung modelo ML2165-W
- Telefonia IP da marca 3CX, com gravação em nuvem e 3 ramais.
- Todos os computadores possuem sistema operacional Windows 10 e pacote Office 365.
- Foram instalados antivírus da marca avast.

11. Revisões e Atualizações

Esta Política será revisada ao menos uma vez a dois anos. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.
A Área de Gestão de Riscos informará oportunamente aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Consultoria na Internet, conforme indicado acima.

ANEXO I

TERMO DE MONITORAMENTO DE GRAVAÇÕES TELEFÔNICAS

Nesta data, _____, foi acessado o arquivo _____ contendo as gravações telefônicas efetuadas pelo ramal _____ e [não] foram identificados indícios que possam indicar eventual infração ao disposto na Política de Segurança das Informações e de Segurança Cibernética e nas demais políticas internas da **Consultoria Financeira.**

São Paulo, [Data]
[Assinatura]

ANEXO II

TERMO DE ADESÃO DE TERCEIRO À POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES E DE SEGURANÇA CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/MF sob o nº _____, declaro que li e estou plenamente de acordo com as disposições da Política de Segurança das Informações e de Segurança Cibernética aprovados pela **CONSULTORIA**. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

São Paulo, [Data]

[Assinatura]