POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DE SEGURANÇA CIBERNÉTICA

Dezembro/2025 – Versão 1.0

VANCOUVER
ASSET MANAGEMENT

Aprovada na Reunião da Diretoria da Vancouver Asset Ltda.
realizada em [dia] de [mês] de 2025

ÍNDICE

1. Apresentação 1
2. Objetivos 1
3. Privacidade e Proteção de Dados Pessoais 2
4. Programa de Segurança da Vancouver 3
5. Monitoramento e Testes Periódicos 12
6. Plano de Resposta 12
7. Vigência e Atualização 13

1. APRESENTAÇÃO

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") da Vancouver Asset Ltda. ("Vancouver" ou "Gestora"), aplica-se a todos os sócios, todos os profissionais, funcionários, terceiros que utilizem o ambiente de processamento da Vancouver, prestadores de serviços e sistemas, bem como aqueles que prestarem trabalhos externamente, ou que acesse informações a ela pertencentes ("Profissionais").

A presente Política foi elaborada em linha com a Resolução da Comissão de Valores Mobiliários nº 21, de 25 de fevereiro de 2021 ("Resolução CVM nº 21/2021").

Todas as diretrizes aqui dispostas são de responsabilidade da Área de *Compliance* da Vancouver, sob a direção do Diretor de *Compliance* da Gestora.

Todos os usuários de recursos computadorizados disponibilizados pela Vancouver têm a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da Vancouver.

2. OBJETIVOS

Esta Política tem por objetivo estabelecer os pilares da segurança, tanto informacional quanto cibernética da Vancouver, determinando medidas a serem tomadas para identificar e prevenir ameaças que possam causar prejuízo à confidencialidade, integridade e disponibilidade de dados e informações necessárias na consecução das atividades da Vancouver.

Em atenção à regulamentação ora aplicável, indicada no item 1 desta Política, a Vancouver procurou identificar, nesta Política, os principais riscos e cenários de ameaça envolvendo os sistemas, dados e processos utilizados pela Vancouver.

Além disso, também buscou analisar as informações e dados de maior sensibilidade referentes à Vancouver ("Informações Confidenciais"), com o propósito de mitigar os riscos da violação de sua confidencialidade.

Também buscou-se determinar, nesta Política, mecanismos e procedimentos para garantir que nenhuma Informação Confidencial seja divulgada a pessoas, vinculadas ou não à

Vancouver, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Vancouver, ou de qualquer natureza relativa às atividades da Gestora e a seus sócios e clientes, obtida em decorrência do desempenho das atividades usuais do Profissional, só poderá ser fornecida ao público, mídia, outras instituições ou demais órgãos caso autorizado previamente e por escrito pelo Diretor de *Compliance* da Vancouver.

3. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Quando um investidor decide adquirir cotas dos fundos de investimentos geridos pela Gestora, dependendo da forma de aquisição das cotas, o tratamento de dados pessoais torna-se necessário para o desempenho das atividades da Gestora, por exemplo, para a execução de rotinas operacionais de investimentos.

A Vancouver não realiza distribuição direta dos seus fundos e, portanto, não têm contato direto com os investidores nesse sentido. A distribuição dos fundos é realizada por meio de distribuidores parceiros, que são os responsáveis pelo contato com o cotista.

Os dados pessoais dos clientes, ainda, podem ser disponibilizados para a Gestora em algumas situações especificas, como, por exemplo, quando há o contato do cotista diretamente por meio dos nossos canais de comunicação (*website*, e-mail, mídias sociais etc.), ou quando é fornecido pelo administrador ou distribuidor do fundo, em situações que exigem a atuação do time operacional das gestoras.

A Vancouver possui, como prática, limitar o tratamento de dados pessoais ao mínimo necessário para execução de suas atividades, abrangendo apenas os dados pertinentes ao processo de suas atividades, de maneira proporcional e não excessiva.

Nesse sentido, os seguintes dados pessoais podem ser tratados pela Gestora: nome, e-mail, foto do seu documento de identidade, geolocalização, filiação, telefone, CPF, RG, endereço físico, protocolo de internet (IP), gênero, estado civil e dados bancários (banco, agência e número da conta).

A Vancouver trata e mantém os dados pessoais tratados somente pelo tempo necessário para cumprir com as finalidades de seu respectivo tratamento, ou seja, pelo período necessário

para execução da sua atividade, enquanto houver uma relação em curso com o titular do dado pessoal ou, ainda, no cumprimento de quaisquer obrigações legais, regulatórias, contratuais, entre outras, desde que fundamentadas legalmente. Após estes períodos, os dados pessoais são eliminados.

Sempre que os cotistas dos fundos sob a sua gestão quiserem tirar dúvidas sobre o tratamento de seus dados pessoais pela Gestora poderá entrar em contato com a Área de *Compliance* da Vancouver, na forma prevista no seu Código de Ética, *Compliance* e Controles Internos.

4. PROGRAMA DE SEGURANÇA DA VANCOUVER

4.1. IDENTIFICAÇÃO DE RISCOS

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.

A Vancouver, na qualidade de gestora de fundos de investimento, conta com servidor de processamento de dados e computadores individuais para todos os seus funcionários e diretores. Além disso, a Vancouver também conta com sistemas referentes às atividades desenvolvidas pela Área de Gestão e sistemas de apoio diversos.

Os métodos mais comuns de ataques cibernéticos são os seguintes:

(i) *malware*: *softwares* desenvolvidos para corromper computadores e redes;

(ii) vírus: *software* que causa danos a máquina, rede, *software*s e banco de dados;

(iii) cavalo de troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;

(iv) *spyware*: *software* malicioso para coletar e monitorar o uso de informações;

(v) *ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido;

(vi) engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito;

(vii) *pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;

(viii) *phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

(ix) *vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

(x) *smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

(xi) acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque;

(xii) ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; e

(xiii) 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 Vancouver pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos ou omissões de seus Profissionais, que podem acarretar a perda e/ou adulteração de dados e Informações Confidenciais.

4.2. AÇÕES DE PREVENÇÃO E PROTEÇÃO

4.2.1. CLASSIFICAÇÃO DO NÍVEL DE SENSIBILIDADE DAS INFORMAÇÕES

Para a prevenção de eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para Vancouver, ao analisar os possíveis impactos financeiros, operacionais e reputacionais que poderão ser sofridos pela Gestora diante da divulgação indevida de tais informações (*i.e.*, em caso de incidente de segurança).

Levando essas questões em consideração, a Vancouver segrega as informações tratadas pela instituição indicando expressamente quando se tratar de dados sigilosos. A depender do nível de confidencialidade da informação, o seu manuseio, armazenamento, transporte e descarte serão realizados de forma diferenciada, conforme determinação da Área de *Compliance*.

4.2.2. CONTROLE DE ACESSO À INFORMAÇÃO

Dentre os procedimentos desenvolvidos pela Vancouver, destaca-se a segregação dos arquivos salvos na rede interna da Vancouver em diferentes diretórios, cujo acesso é limitado a determinados Profissionais que possuem a devida autorização de acesso, conforme usuário e senha pessoal de cada Profissional.

A Vancouver destaca que a determinação das restrições de acesso foi realizada considerando: (i) a área de atuação de cada Profissional; e (ii) o conteúdo dos arquivos que estão presentes em cada um dos diretórios. Desse modo, as informações acessíveis por cada Profissional são aquelas relativas ou à sua respectiva área, ou aquelas que não estejam diretamente relacionados a sua função, mas que sejam relevantes para o exercício da sua atividade.

Sempre que novos diretórios são criados essa análise de adequação é novamente realizada pela Área de *Compliance*.

Apenas o Diretor de *Compliance* possui acesso a todos os diretórios da rede, bem como a todos os *desktops* pessoais dos Profissionais, de modo a viabilizar a análise de qualquer documento que possa potencialmente violar as normas regulamentares e legais aplicáveis à Vancouver.

Todos os Profissionais Internos (cf. abaixo definido) poderão ter acesso remoto, por meio de seus dispositivos pessoais, aos diretórios que tiverem acesso.

4.2.3. DEFINIÇÃO DE SENHAS DE ACESSO A DISPOSITIVOS E SISTEMAS CORPORATIVOS

As senhas utilizadas pelos Profissionais, para acesso a qualquer sistema disponibilizado pela Vancouver, serão invioláveis e intransferíveis, não podendo ser reveladas a outra pessoa.

Além disso, as senhas deverão ser atualizadas a cada 60 dias, atendendo sempre um critério de complexidade que será indicado no momento de definição da senha.

4.2.4. PROPRIEDADE DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Todos os recursos computacionais de *hardware* disponibilizados para os Profissionais são de propriedade da Vancouver, sendo permitida a utilização de *notebooks*, *tablets* ou outros *hardwares*, sendo eles pessoais ou não, para a realização de atividades relacionadas a sua função na Vancouver, desde que o Diretor de *Compliance* seja informado a esse respeito.

4.2.5. DISPONIBILIZAÇÃO E USO

Todos os computadores e *softwares* disponibilizados para os Profissionais da Vancouver têm por objetivo o desempenho das atividades profissionais referentes à Vancouver, não devendo ser utilizado para quaisquer outros fins.

Todo o processo de criação e exclusão de usuário, instalação de *software*s e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados por prestadores de serviços terceirizados, especializados em tecnologia da informação, contratados pela Vancouver, mediante aprovação do Diretor de *Compliance*.

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

(i) a cada novo Profissional, o Diretor de *Compliance* autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;

(ii) todos os equipamentos, *software*s e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão e aprovação do Diretor de *Compliance*;

(iii) o Diretor de *Compliance* autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;

(iv) 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 Diretor de *Compliance*;

(v) a identificação do usuário é feita por meio de *login* e senha; e

(vi) todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de *Compliance* à área responsável.

4.2.6. *SOFTWARES*

A implantação e configuração de *software*s da Vancouver respeitam as seguintes regras:

(i) todos os *software*s, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável, mediante supervisão e aprovação do Diretor de *Compliance;*

(ii) é desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada do Diretor de *Compliance*;

(iii) é desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores; e

(iv) a conexão de dispositivos móveis de armazenamento (e.g. *USB Drive*) somente poderá ser realizada mediante autorização prévia e expressa do Diretor de *Compliance*.

4.2.7. PROTEÇÃO

A Vancouver se responsabiliza a instalar, em todos os dispositivos disponibilizados aos Profissionais Internos (cf. definido abaixo) sistemas de *firewalls* e recursos *anti-malware*. Estes últimos também serão disponibilizados aos dispositivos pessoais dos Profissionais

Internos que, eventualmente, poderão ser utilizados para atividades referentes às suas respectivas funções.

4.2.8. REGISTROS

A Vancouver mantém por 5 anos todos os *logs* de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam *softwares*, *hardwares* ou acessos que não sejam autorizados.

Nesse sentido, por meio dos *logs* realizados pela Vancouver, a Gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme determina a Resolução CVM nº 21/2021.

4.2.9. REGRAS E RESPONSABILIDADES DO USO DA INTERNET

O Profissional é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar por meio de recursos de tecnologia da Vancouver, este deve sempre resguardar a imagem da Vancouver, evitando entrar em sites de fontes não seguras, assim como de abrir *e-mails* pessoais, ou, de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo Diretor de *Compliance*.

O usuário é proibido de acessar sítios eletrônicos que:

(i) possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes;

(ii) possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;

(iii) contenham informações que não colaborem para o alcance dos objetivos da Vancouver;

(iv) defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física; e

(v) possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem *links* suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

4.2.10. USO DE CORREIO ELETRÔNICO PARTICULAR

É proibida a utilização profissional de correio eletrônico particular.

A Vancouver disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais (ex.: [nome do funcionário@vancouverasset.com.br]).

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

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

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

4.2.11. ENDEREÇO ELETRÔNICO DE PROGRAMAS OU DE COMUNICAÇÃO CORPORATIVA

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico atribuível aos funcionários e diretores da Vancouver ("Profissionais Internos"). Nesse caso, é obrigatória a existência de um usuário da Área de *Compliance* responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.

É permitida a existência de endereços de correio eletrônico para o envio de mensagens referentes à Comunicação Interna entre os Profissionais Internos. Sempre será obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado aos Profissionais Internos e as mensagens associadas ao seu respectivo correio eletrônico são de propriedade da Vancouver. No

entanto, os Profissionais Internos serão exclusivamente responsáveis pelo conteúdo das mensagens encaminhadas por meio do referido correio eletrônico.

No caso de recebimento de mensagens cuja higidez seja questionável, o Profissional Interno que tiver obtido acesso à tal mensagem deverá cientificar ao membro da Área de *Compliance* responsável pelo acompanhamento de mensagens. Após a sua análise, caso conclua que tal mensagem represente alguma ameaça ao sistema e às informações da Vancouver, deverá encaminhar e-mail a todos Profissionais Internos com a mensagem suspeita, indicando que, caso recebam e-mail com conteúdo semelhante, deverão prosseguir com a sua exclusão.

4.2.12. RESPONSABILIDADES E FORMA DE USO DE CORREIO ELETRÔNICO

O Profissional que utiliza um endereço de correio eletrônico disponibilizado pela Vancouver é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu *e-mail*, podendo enviar mensagens necessárias para o seu desempenho profissional na Gestora.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

(i) contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;

(ii) façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;

(iii) menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;

(iv) possuam informação pornográfica, obscena ou imprópria para o ambiente profissional;

(v) sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;

(vi) defendam ou possibilitem a realização de atividades ilegais;

(vii) sejam ou sugiram a formação ou divulgação de correntes de mensagens;

(viii) possam prejudicar a imagem da Vancouver; e

(ix) sejam incoerentes com esta Política e/ou com as demais regras e procedimentos internos da Vancouver.

O Profissional que tiver correio eletrônico disponibilizado pela Gestora deve estar ciente que uma mensagem de correio eletrônico da Vancouver é um documento formal e, portanto, deverá ser tratado como um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, atribuindo-lhe à opinião da Vancouver.

O Profissional deve ser diligente em relação:

(i) aos usuários que receberão a mensagem (destinatário/copiado/copiado oculto);

(ii) ao nível de sigilo da informação contida na mensagem e, conforme o caso, avaliar a necessidade de indicação expressa do grau de confidencialidade da informação;

(iii) aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e indicando, de forma clara e inquestionável, a confidencialidade dos mesmos; e

(iv) ao uso da opção "encaminhar", verificando se é necessária a manutenção das diversas mensagens anteriores que estão encaminhadas.

4.2.13. ARMAZENAMENTO EM "NUVEM" (*CLOUD*)

A Vancouver poderá realizar o armazenamento das Informações Confidenciais e quaisquer outros dados na "nuvem" (*cloud*), desde que seja realizado por uma empresa de alto renome e capacidade.

Além disso, a Área de *Compliance* será responsável por diligenciar a empresa que será contratada, avaliando se a referida empresa demonstra atender critérios de confidencialidade e de segurança.

Caso a Vancouver contrate sistema de "nuvem", serão adotadas as medidas necessárias para que os Profissionais tenham acesso remoto, por meio de seus dispositivos pessoais, à rede de armazenamento na "nuvem".

4.3. CONTINUIDADE DAS ATIVIDADES

Para garantir a continuidade das atividades da Vancouver, será feito *backup* das informações digitais e dos sistemas existentes nos dispositivos disponibilizados pela Vancouver aos Profissionais, por meio dos seguintes processos:

(i) *backup* executado diariamente;

(ii) manutenção dos sistemas em funcionamento, apesar de falta de energia temporária, por meio de equipamentos de *no break* instalados para suprir o fornecimento de energia nos equipamentos principais para a manutenção das comunicações e atividades mínimas da Vancouver; e

(iii) manutenção de meios remotos seguros para o trabalho de seus Profissionais.

5. MONITORAMENTO E TESTES PERIÓDICOS

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela Área de *Compliance*. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Vancouver 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 Vancouver.

6. PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a Vancouver desenvolveu Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Caso seja verificada uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política.

São indicadas, abaixo, as medidas que deverão ser adotadas pela Área de *Compliance* nesses casos:

(i) criação de laudo contendo as informações que foram potencialmente vazadas;

(ii) desinstalação de *software*;

(iii) execução de varreduras *offline* para descobrir quaisquer ameaças adicionais;

(iv) substituição física de dispositivos de armazenamento sempre que se demonstrar necessário;

(v) restauração de dados provenientes do *backup* realizado diariamente;

(vi) criação de relatório baseado no laudo elaborado, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança; e

(vii) em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido.

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

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 ser formalizado no Relatório de Controles Internos da Vancouver.

Caso o evento tenha sido causado por algum Profissional, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da Vancouver.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente pela Área de *Compliance*. Caso seja constatada necessidade de alteração do seu conteúdo (seja em decorrência da revisão anual ou da verificação espontânea da necessidade de alteração, a qualquer tempo), a Área de

Compliance submeterá à aprovação dos demais administradores da Vancouver as alterações propostas à Política.