MANUAL DE COMPLIANCE

PROPÓSITO

O objetivo deste Manual de Compliance ("Manual") da **VIGM, S.A. de C.V. Asesor en Inversiones Independiente** ("Consultora") é estabelecer os princípios fundamentais, normas e procedimentos que orientam o tratamento seguro, responsável e ético das informações utilizadas nas atividades de consultoria de investimentos da Consultora para Clientes residentes e domiciliados no Brasil ("Clientes"). Ao estabelecer expectativas claras, a Consultora promove a integridade, a transparência e a responsabilidade na gestão das informações e dos recursos tecnológicos.

Ao aderir a este Manual, os Colaboradores e prestadores de serviços contribuem para a proteção dos interesses dos Clientes e da Consultora, asseguram um ambiente operacional seguro e apoiam uma cultura de profissionalismo e conduta ética no tratamento de informações sensíveis.

ESCOPO

Este Manual aplica-se a todos os profissionais empregados pela Consultora que atuam nas áreas de consultoria de valores mobiliários, controles internos e compliance da Consultora, incluindo, sem limitação, quaisquer diretores, administradores, gerentes, empregados, trabalhadores temporários, estagiários e aprendizes, bem como outras pessoas que possuam status semelhante ou desempenhem funções similares ("Colaboradores").

1. INTRODUÇÃO

Este Manual deve ser lido em conjunto com o Código de Ética e as demais políticas da Consultora.

2. DEFINIÇÕES

Todos os termos iniciados com letras maiúsculas que não forem aqui definidos têm seu significado atribuído no Código de Ética da Consultora.

3. PROTEÇÃO DAS INFORMAÇÕES DE PROPRIEDADE EXCLUSIVA DA EMPRESA E DO CLIENTE

3.1. Procedimentos para Divulgação Adequada de Informações

A Consultora frequentemente coleta dados ou informações que podem ser utilizados isoladamente ou em conjunto com outras informações para distinguir ou rastrear a identidade de um indivíduo, tais como nome, número de CPF, data e local de nascimento, nome de solteira da mãe ou registros biométricos ("Informações Pessoais") diretamente de indivíduos, como clientes atuais e potenciais. A Consultora também pode coletar Informações Pessoais sobre indivíduos de suas coligadas e/ou de terceiros. Em cada caso, a coleta e o uso de tais Informações Pessoais pela Consultora deverão estar em conformidade com os termos de qualquer aviso aplicável que a Consultora possa fornecer a tais indivíduos.

A Consultora poderá divulgar Informações Pessoais a terceiros em diversas circunstâncias. Primeiramente, a Consultora poderá ser obrigada a divulgar Informações Pessoais a terceiros para cumprir uma obrigação legal, como em resposta a uma intimação judicial, ou a um regulador no contexto de um exame regulatório. Além disso, a Consultora poderá compartilhar Informações Pessoais com terceiros que não sejam coligadas, como um fornecedor terceirizado. Em ambos os casos, os Colaboradores deverão adotar medidas razoáveis e apropriadas para proteger tais Informações Pessoais.

Quaisquer comunicações recebidas de autoridades governamentais, regulatórias ou autorreguladoras deverão

ser prontamente encaminhadas ao Diretor de Compliance para o tratamento adequado.

Os Colaboradores não poderão divulgar informações sobre recomendações ou possíveis operações que ainda não tenham sido formalizadas ou que estejam em análise, exceto **(i)** quando necessário para o desempenho de suas atividades profissionais; ou **(ii)** quando exigido por lei (neste caso, mediante notificação ao Diretor de Compliance – por e-mail); e **(iii)** após a informação estar disponível ao público.

A Consultora possui como dever primordial a lealdade a todos os investidores, notadamente seus Clientes. Esse dever inclui a não apropriação indevidamente de informações e/ou estratégias desenvolvidas para a elaboração de recomendações de investimento com o objetivo de utilizá-las em negociações pessoais (ou negociações para outras contas) de tais Colaboradores. De maneira geral, as políticas de negociação pessoal da Consultora presentes no referido Código de Ética devem prevenir tal apropriação indevida, mas se qualquer Colaborador acreditar que está em posição de lucrar com o uso de informações específicas que tenha recebido ou que tenham sido geradas no contexto das atividades realizadas pela Consultora, tal Colaborador não deverá executar a operação em questão. Assim, em consonância com as políticas internas da Consultora.

4. TRATAMENTO DE DADOS

4.1. Titularidade dos Dados

Exceto por materiais claramente pertencentes a terceiros, tais como seus dados pessoais confidenciais, a Consultora é a legítima proprietária de todas as informações comerciais armazenadas ou transmitidas por meio de seus sistemas. Salvo se a Consultora tiver celebrado um acordo escrito específico, todas as informações comerciais desenvolvidas enquanto um Colaborador estiver empregado pela Consultora são de propriedade da Consultora.

Os Colaboradores, fornecedores e quaisquer outros terceiros não poderão copiar os softwares e/ou arquivos fornecidos pela Consultora em qualquer meio de armazenamento, transferir tais softwares e/ou arquivos para outro computador ou divulgar tais softwares e/ou arquivos a terceiros externos sem autorização prévia do Diretor de Compliance.

4.2. Limitação de Informações Pessoais

A Consultora envidará todos os esforços razoáveis para limitar **(i)** a quantidade de informações coletadas dos Clientes e/ou obtidas no contexto de suas atividades de consultoria no Brasil ao que for razoavelmente necessário para atingir a finalidade legítima para a qual foram coletadas; **(ii)** o período de retenção de tais informações ao que for razoavelmente necessário para atingir tal finalidade; e **(iii)** o acesso às pessoas que razoavelmente necessitem conhecer tais informações para atingir tal finalidade ou para cumprir requisitos estaduais ou federais de retenção de registros.

5. TREINAMENTO

Como parte de seu programa de controles internos, a Consultora fornecerá treinamento sobre este Manual a todos os Colaboradores e, se necessário, a coligadas e fornecedores. O treinamento pode ser realizado por meio de reuniões corporativas, distribuição de materiais escritos ou orientações fornecidas por e-mail. O Diretor de Compliance será responsável por manter um registro de quaisquer orientações ou materiais escritos fornecidos durante tais treinamentos.

O treinamento é realizado sempre que o Diretor de Compliance julgar necessário e no momento da integração de um novo Colaborador, conforme explicado abaixo.

5.1. Treinamento de Integração:

Novos colaboradores deverão participar de atividades de conscientização e treinamento em segurança cibernética como parte do processo de admissão.

5.2. Treinamento contínuo

A educação contínua em segurança cibernética deverá ser conduzida para os Colaboradores apropriados, no mínimo anualmente, para garantir que estejam cientes da importância da segurança cibernética. A conscientização e o treinamento em segurança cibernética deverão incluir tópicos como táticas de engenharia social (por exemplo, *phishing*) e outras ameaças cibernéticas relevantes que possam levar ao comprometimento de sistemas e/ou à perda de dados.

6. SEGURANÇA DA INFORMAÇÃO

O Programa de Segurança Empresarial da Consultora é um programa gerenciado globalmente e baseado em riscos, concebido para proteger a confidencialidade, a integridade e a disponibilidade das informações de clientes, funcionários e da empresa, ao mesmo tempo em que apoia os objetivos comerciais da Consultora. O programa opera sob a supervisão do Conselho de Administração e é liderado pelo Diretor de Segurança da Informação (CISO), responsável por sua concepção, implementação e operação contínua. A execução é realizada por meio de uma organização de Segurança Empresarial, que estabelece a estratégia, as políticas, os padrões e as atividades de garantia de segurança em toda a empresa. O programa é orientado por estruturas reconhecidas do setor, como a Estrutura de Cibersegurança do NIST, e outras práticas de ponta, e integra a gestão de riscos de cibersegurança aos processos mais amplos de gestão de riscos corporativos da Consultoria. Por meio de governança centralizada, padrões globalmente consistentes, monitoramento contínuo e relatórios regulares à alta administração e aos conselhos, o programa possibilita uma postura de segurança resiliente que se adapta às ameaças em constante evolução, mantendo a conformidade regulatória e a prontidão para auditorias.

6.1. Estrutura de Gestão de Riscos

6.1.1. Avaliações de riscos de segurança cibernética

A Consultora realiza avaliações de riscos de segurança cibernética periodicamente e em resposta a mudanças ou eventos significativos que possam afetar os sistemas, dados ou serviços que dão suporte às atividades regulamentadas. Essas avaliações levam em consideração ameaças e vulnerabilidades relevantes, a sensibilidade e a criticidade das informações e dos serviços, bem como o potencial impacto nos negócios e nos clientes.

Os riscos identificados são documentados, atribuídos a um responsável e tratados por meio de ações de tratamento de riscos (por exemplo, mitigação, transferência ou aceitação) alinhadas à governança da Consultora. Os riscos que excedam os limites de tolerância definidos, envolvam impacto significativo nos negócios ou exijam decisões da administração são encaminhados imediatamente por meio de processos estabelecidos de relatório e tomada de decisão

Os Colaboradores devem entender que os sistemas de informação, redes, dispositivos e ferramentas de comunicação fornecidos ou aprovados pela Consultora são destinados ao uso comercial e são de propriedade da Consultora. Na medida permitida pela legislação aplicável, os Colaboradores não devem ter expectativa de privacidade ao utilizar esses sistemas. Para proteger a segurança, integridade e funcionamento adequado de seus sistemas de informação, e para cumprir obrigações legais, regulatórias

e de políticas internas, a Consultora poderá monitorar, registrar, acessar, revisar e utilizar informações criadas, armazenadas, transmitidas ou recebidas por meio de seus sistemas de informação. Tais atividades podem incluir, quando apropriado, a revisão de comunicações eletrônicas, dados de uso do sistema, registros de acesso e outras informações geradas por meio do uso dos sistemas da Consultora.

6.1.2. Gestão de ameaças e vulnerabilidades

A Consultora mantém processos para identificar ameaças à segurança cibernética e vulnerabilidades que possam afetar significativamente as atividades regulamentadas, utilizando informações relevantes sobre ameaças e vulnerabilidades (por exemplo, alertas de fornecedores e atualizações de segurança), conforme apropriado. As vulnerabilidades identificadas são avaliadas e priorizadas com base no risco, levando em consideração a probabilidade, a exposição e o potencial impacto nos negócios e nos clientes. As medidas corretivas são acompanhadas e implementadas em tempo hábil, de acordo com o nível de risco.

6.2. Identidade, Autenticação e Gerenciamento de Acesso

6.2.1. Princípios de Controle de Acesso

A Consultora mantém controles de acesso projetados para garantir que o acesso a sistemas e informações seja autorizado e concedido com base no mínimo privilégio e na necessidade de saber, em conformidade com as responsabilidades definidas do negócio.

O acesso é provisionado, modificado e removido com base em autorização documentada e aprovação apropriada. Os direitos de acesso são revisados periodicamente e ajustados prontamente para refletir mudanças em funções, responsabilidades ou necessidades do negócio.

6.2.2. Autenticação e Gerenciamento de Senhas

A Consultora usa controles de autenticação para identificar exclusivamente os usuários e verificar sua identidade antes de conceder acesso aos seus sistemas e informações. Os requisitos de senha e autenticação (por exemplo, padrões de senha segura, proteção de credenciais e controles de conta) são mantidos para reduzir o risco de acesso não autorizado. Quando justificado com base na sensibilidade do sistema, dos dados ou do canal de acesso, a Consultora aplica autenticação mais forte, como autenticação multifator

6.2.3. Acesso Remoto

O acesso remoto aos sistemas da Consultora é permitido somente quando autorizado e é controlado por meio de métodos e configurações aprovados, projetados para proteger sistemas e informações. Espera-se que os usuários se conectem de forma segura e cumpram os requisitos aplicáveis de conectividade remota (por exemplo, uso de dispositivos e redes aprovados, conexões remotas seguras e proteção de credenciais). A atividade de acesso remoto está sujeita a supervisão, registro e monitoramento, com revisão periódica para confirmar a adequação contínua. A autenticação multifator é exigida para acesso remoto.

6.3. Controles de Proteção de Dados e Sistemas

6.3.1. Criptografia e Proteção de Informações

A Consultora aplica salvaguardas para proteger informações sensíveis em trânsito (por exemplo, durante a transmissão por redes) e em repouso (por exemplo, quando armazenadas em sistemas ou mídias), incluindo criptografia quando apropriado. A seleção e a força da criptografia, e quaisquer controles compensatórios quando a criptografia não for viável, são aplicados com base em risco, considerando a sensibilidade dos dados,

as expectativas regulatórias, a arquitetura do sistema e os requisitos de negócio.

6.3.2. Dispositivos Móveis

Dispositivos móveis e portáteis usados para fins comerciais ou para acessar sistemas ou informações da Consultora devem ser usados de acordo com os requisitos de segurança da Consultora (por exemplo, uso de configurações aprovadas, conectividade segura e proteção de credenciais e dados). Salvaguardas apropriadas são implementadas para mitigar riscos associados a perda, roubo ou acesso não autorizado. O uso de dispositivos pessoais ou de terceiros para fins comerciais é permitido somente quando autorizado e sujeito aos requisitos de segurança aplicáveis.

6.4. Uso Aceitável, Privacidade e Responsabilidades dos Funcionários

6.4.1. Acesso à Internet e Uso Aceitável

O acesso à internet é fornecido para apoiar fins comerciais legítimos e deve ser usado de acordo com os requisitos de uso aceitável da Consultora, incluindo usos aceitáveis e proibidos definidos dos sistemas e recursos da Consultora. Usos proibidos incluem atividades que sejam ilegais, inadequadas ou que possam comprometer a segurança, confidencialidade ou disponibilidade do sistema. Controles são aplicados para reduzir a exposição a conteúdo malicioso ou inadequado (por exemplo, filtragem da web e proteções de segurança relacionadas) e para ajudar a detectar e prevenir o uso indevido dos recursos da Consultora.

6.4.2 Privacidade dos Funcionários e Uso Pessoal de Sistemas

A Consultora equilibra as obrigações de segurança da informação e regulatórias com o respeito à privacidade dos funcionários. O monitoramento, acesso e revisão dos sistemas e informações da Consultora são conduzidos de maneira destinada a ser proporcional e consistente com a lei aplicável, requisitos regulatórios e necessidades de segurança.

O pessoal é informado de que os sistemas da Consultora (incluindo rede, e-mail, uso da internet e outros recursos tecnológicos) podem ser monitorados e registrados para proteger a segurança, gerenciar risco e apoiar o compliance regulatório. Quando o uso pessoal limitado for permitido, ele deve ser incidental, não deve interferir nas atividades comerciais e deve cumprir este Manual e as políticas relacionadas da Consultora.

6.5. Monitoramento e Detecção de Segurança

A Consultora monitora sistemas e atividade dos usuários de forma apropriada ao seu perfil de risco para apoiar a detecção de comportamento anômalo ou suspeito e indicadores de possíveis eventos de cibersegurança ou violações de políticas. Registros e alertas de monitoramento são usados para apoiar a investigação, escalonamento e resposta tempestivos a possíveis incidentes.

6.6. Gestão de Incidentes de Cibersegurança

A Consultora mantém uma capacidade de resposta a incidentes destinada a permitir a identificação, contenção, erradicação e recuperação tempestivas de incidentes de cibersegurança, ao mesmo tempo em que reduz potenciais danos aos Clientes, à Consultora e às atividades reguladas. A resposta a incidentes é coordenada, conforme apropriado, com processos de continuidade de negócios e gestão de crises para apoiar a continuidade de serviços críticos, comunicações internas e externas eficazes e escalonamento à administração quando impactos operacionais mais amplos forem previstos.

Um incidente de cibersegurança declarado é um evento de segurança que é escalonado para Nível de Crise e

aciona o plano da Equipe de Resposta a Incidentes de Segurança da Informação (ISIRT) e a Resposta a Crises Corporativas. Todos os incidentes de segurança seguem um caminho de escalonamento baseado na criticidade e no risco geral para a Consultora.

6.6.1. Identificação, Escalonamento e Reporte de Incidentes

Incidentes de cibersegurança são identificados, avaliados e classificados com base na gravidade, escopo e potencial impacto à Consultora, aos Clientes e às atividades reguladas. Eventos suspeitos são escalonados prontamente por meio de caminhos internos de escalonamento ao Diretor de Compliance e outros tomadores de decisão designados com autoridade para direcionar ações de resposta, aprovar comunicações e determinar obrigações de reporte. Quando um incidente atingir os limites aplicáveis de notificação regulatória, a Consultora fará os reportes regulatórios exigidos, incluindo notificação à CVM, de acordo com os requisitos aplicáveis e procedimentos internos.

6.6.2. Fases de Resposta a Incidentes de Cibersegurança

As atividades de resposta a incidentes seguem um ciclo de vida estruturado que inclui identificação e análise, contenção e mitigação, recuperação dos serviços afetados e revisão e melhoria pós-incidente.

6.6.3. Plano de Resposta a Incidentes de Cibersegurança

A Consultora mantém um plano formal e documentado de resposta a incidentes de cibersegurança, regido por supervisão estabelecida, incluindo papéis e responsabilidades definidos. O plano é mantido e revisado periodicamente, e é testado conforme apropriado, para confirmar a eficácia contínua e incorporar lições aprendidas, mudanças materiais em sistemas e operações, e ameaças e expectativas regulatórias em evolução.

6.7. Seguro de Cibersegurança

Seguro de cibersegurança pode ser usado como medida suplementar de gestão de risco. A existência de tal cobertura não reduz nem substitui a obrigação da Consultora de manter controles eficazes de cibersegurança e capacidades de resposta.

6.8. Treinamento e Conscientização em Cibersegurança

6.8.1. Treinamento de Segurança em Cibersegurança

A Consultora mantém um programa de treinamento e conscientização em segurança da informação que estabelece expectativas para que o pessoal compreenda e cumpra as políticas de segurança aplicáveis, reconheça riscos relevantes de cibersegurança e execute suas responsabilidades para proteger sistemas e informações.

Os funcionários recebem treinamento inicial em segurança da informação como parte da integração e, posteriormente, atividades contínuas de treinamento e conscientização, que reforçam políticas-chave, ameaças emergentes e responsabilidades individuais. O conteúdo do treinamento pode ser adaptado, quando apropriado, com base na função, privilégios de acesso e exposição a informações sensíveis.

6.9. Testes e Monitoramento de Controles

A Empresa mantém um programa baseado em risco para o teste e monitoramento contínuo de seus controles internos, incluindo controles que apoiam compliance, integridade operacional e cibersegurança. Os controles são periodicamente avaliados para confirmar que são adequadamente desenhados e operam efetivamente,

usando metodologias documentadas e repetíveis proporcionais à natureza, tamanho e complexidade das atividades e perfil de risco da Empresa. Atividades de monitoramento são realizadas para apoiar a identificação tempestiva de falhas, deficiências ou riscos emergentes, e os resultados são documentados, escalonados conforme apropriado e sujeitos a ação corretiva. Evidências de testes, monitoramento e remediação são mantidas de maneira verificável para apoiar a supervisão da administração, revisão independente e supervisão regulatória.

7. TREINAMENTO

Como parte de seu programa de controles internos, a Consultora fornecerá treinamento sobre este Manual a todos os Funcionários e, se necessário, a afiliadas e fornecedores. O treinamento pode assumir a forma de reuniões em toda a empresa, distribuição de materiais escritos ou orientação fornecida por e-mail. O Diretor de Compliance será responsável por manter um registro de qualquer orientação ou materiais escritos fornecidos durante tal treinamento.

O treinamento é realizado sempre que o Diretor de Compliance considerar necessário e no momento da integração de

8. VIOLAÇÃO

A violação deste Manual poderá resultar na aplicação pelo Diretor de Compliance das sanções que julgar apropriadas, incluindo, mas não se limitando a, carta de censura, suspensão ou rescisão do contrato de trabalho do infrator. A Consultora reserva-se o direito de notificar as autoridades policiais competentes sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade.

9. DISPOSIÇÕES GERAIS

Este Manual está disponível no website da Consultora, em conformidade com o Artigo 14, inciso III, da Resolução CVM nº 19.

10. PRAZO E ATUALIZAÇÃO

Este Manual será revisado anualmente pela Consultora e será alterado sempre que houver necessidade de atualização de seu conteúdo.