INTRA DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA.
("TECNOLOGIA DA INFORMAÇÃO")

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA
("POLÍTICA")

JULHO/2024

Sumário

1. Política de Segurança da Informação e Segurança Cibernética

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da Administradora e às disposições deste Manual, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações da Administradora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

Todos os equipamentos da rede deverão estar acomodados em uma sala fechada, de acesso restrito. As estações de trabalho serão fixas, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Administradora.

A execução direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Diretoria Compliance que, em conjunto com a equipe de Tecnologia da Informação serão responsáveis inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme descrito neste Manual.

1.1 Identificação de Riscos (risk assessment)

No âmbito de suas atividades, a Administradora identificou os seguintes principais riscos internos e externos que precisam de proteção:

(i) Dados e Informações: Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Administradora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua administração, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

(ii) Sistemas: Informações sobre os sistemas utilizados pela Administradora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

(iii) Processos e Controles: Processos e controles internos que sejam parte da rotina das áreas de negócio da Administradora; e

(iv) Governança da Gestão de Risco: Eficácia da gestão de risco pela Administradora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Administradora identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

(i) Malware – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware e Ransomware);

(ii) Engenharia social – métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);

(iii) Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e

(iv) Invasões (advanced persistent threats): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no item acima, a Administradora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

1.2 Ações de Prevenção e Proteção

Após a identificação dos riscos, a Administradora adota as medidas a seguir descritas para proteger Informações Confidenciais e sistemas.

• Regra Geral de Conduta

A Administradora realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os colaboradores circulem em ambientes externos à Administradora com arquivos utilizados, gerados ou disponíveis na rede da Administradora, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Administradora. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a Informação Confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os colaboradores da Administradora deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a Equipe de Compliance deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Administradora qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Administradora.

A Administradora também mantém arquivo físico centralizado, porém, cada Colaborador é o responsável pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham Informações Confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com a política de segurança, é proibido aos colaboradores, o uso de pen-drivers, fitas, discos ou quaisquer outros meios de gravação. É proibida a conexão de equipamentos na rede da Administradora que não estejam previamente autorizados pela área de informática e pelos administradores da Administradora.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da Administradora.

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, de modo que estas permaneçam o menor tempo possível nos computadores da Administradora.

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

Ações de Prevenção e Proteção de Informações Confidenciais e Segurança Cibernética	
Acesso Escalonado do Sistema	O acesso como “administrador” de área de *desktop* é limitado aos usuários aprovados pelo Diretor de Compliance e área de TI e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores. A Administradora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Administradora necessária ao exercício de suas atividades. A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Administradora em caso de violação.

Senha e Login	A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas trimestralmente, conforme aviso fornecido pelo responsável pela área de informática. Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.
Uso de Equipamentos e Sistemas	Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. A utilização dos ativos e sistemas da Administradora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional. Todo colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar a Diretoria de Compliance
Acesso Remoto	A Administradora permite o acesso remoto pelos colaboradores ao e-mail, rede e diretório, conforme requisição por estes e autorização pela Diretoria de Compliance e área de TI, através de notebooks fornecidos pela mesma. Ademais, os colaboradores autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (iii) relatar a Diretoria de Compliance qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Administradora e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

Controle de Acesso	O acesso de pessoas estranhas à Administradora a áreas restritas somente é permitido com a autorização expressa de colaboradores autorizados pelos administradores da Administradora. Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos colaboradores, a Administradora monitora a utilização de tais meios.
Firewall, Software, Varreduras e Backup	A Administradora utiliza um hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. A Diretoria de Compliance em conjunto com a área de TI, são responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede). A Administradora mantém proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, vírus, worms, spyware). Serão conduzidas varreduras diárias para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Administradora. A Administradora utiliza um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e patches. A área de TI, de acordo política de segurana, é responsável por patches regulares nos sistemas da Administradora. A Administradora mantém e testa regularmente medidas de backup consideradas apropriadas conforme política interna e estrutura da Administradora. As informações da Administradora são atualmente objeto de backup **diário** com o uso de computação na nuvem.

1.3 Monitoramento e Testes

A Equipe de Compliance, adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, anualmente.

(i) Monitoramento, por amostragem, do acesso dos colaboradores a sites, blogs,fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;

(ii) Monitoramento, por amostragem, das ligações telefônicas dos seus colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Administradora para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da Administradora; e

(iii) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

(iv) Monitoramento dos e-mails transacionados através do sistema Arkiv mail.

A Equipe de Compliance, poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

1.4 Plano de Identificação e Resposta

• Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Administradora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada a Diretoria de Compliance prontamente. A Diretoria de Compliance em conjunto com o comitê executivo, determinará quais membros da administração da Administradora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.
Ademais, determinarão quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

• Procedimentos de Resposta

O comitê executivo em conjunto com a Diretoria de Compliance e área de TI, responderão a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Administradora de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;
(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo

de investimento sob administração da Administradora, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
(vii) Determinação do responsável (ou seja, a Administradora ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Comitê Executivo, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

1.5 Arquivamento de Informações

Os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, bem como todos os documentos e informações exigidos pela Resolução CVM nº 21, correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções em conformidade com o inciso IV do Artigo 18 e com o Artigo 34 da Resolução CVM nº 21.

2. Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Administradora, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Administradora, razão pela qual o colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Administradora, devendo todos os documentos permanecer em poder e sob a custódia da Administradora, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Administradora, salvo se autorizado expressamente pela Administradora e ressalvado o disposto abaixo.

Caso um colaborador, ao ser admitido, disponibilize à Administradora documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à Administradora, o colaborador deverá assinar declaração nos termos do Anexo III ao presente Manual, confirmando que:

(i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e

(ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Administradora, sendo que o colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Administradora, exceto se aprovado expressamente pela Administradora.

3. Descarte de Software

A **INTRA DTVM** realizou a implementação desta política segregada para o descarte de software, após observarmos o quão fundamental é para proteger os ativos de informação da organização contra possíveis violações de segurança. (ANEXO II)

ANEXO I
TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____, doravante denominado Colaborador, e **INTRA DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA.**, inscrita no CNPJ sob o nº 15.489.568/0001-95 ("Administradora").
Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Administradora, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Administradora, seus sócios e clientes, aqui também contemplados os próprios fundos, incluindo:

   a) *Know-how,* técnicas, cópias, diagramas, modelos, amostras, programas de computador;

   b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos fundos de investimento e carteiras administradas pela Administradora;

   c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento administradas pela ADMINISTRADORA;

   d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, *trainees* ou estagiários da Administradora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (*IPO*), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Administradora e que ainda não foi devidamente levado à público;

   e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;

   f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

   g) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees* ou estagiários da Administradora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

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

2.1. O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Administradora, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "*Insider Trading*", "Dicas" e "*Front Running*", seja atuando em benefício próprio, da Administradora ou de terceiros.
A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e crimina

2.2. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Administradora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.
O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

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

3. O Colaborador reconhece e toma ciência que:

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

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

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Administradora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de

informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

4. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Administradora, permitindo que a Administradora procure a medida judicial cabível para atender ou evitar a revelação. 5.1. Caso a Administradora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

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

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

6. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Administradora. Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

São Paulo, _____

_____
COLABORADOR

_____
INTRA DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA.

Testemunhas:

1.
Nome:
CPF/ME:

2.
Nome:
CPF/ME:

ANEXO II

INTRA DTVM - POLÍTICA DE DESCAI

4. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada **anualmente**, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

Histórico das atualizações			
Data	**Versão**	**Responsável**	**Aprovação**
Maio de 2022	v.2	Diretor de *Compliance*, Risco Operacional e PLD-FTP	Comitê de *Compliance*
Abril de 2023	v.3	Diretor de *Compliance*, Risco Operacional e PLD-FTP	Comitê de *Compliance*
Junho de 2024	v.4	Diretor de *Compliance*, Risco Operacional e PLD-FTP	Comitê de *Compliance*