POLÍTICA, PROCESSO E PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA E SEGURANÇA DA INFORMAÇÃO

CV INVESTIMENTOS DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA.

Novembro de 2024.

ÍNDICE

1. OBJETIVO

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") é a declaração formal da **CV INVESTIMENTOS DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA.** ("CV DTVM"), acerca de seu compromisso com as medidas de segurança da informação e as ameaças aos negócios, buscando, principalmente, mas não exclusivamente, a proteção de informações confidenciais.

A Política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco e modelo de negócios da CV DTVM. Esta Política foi elaborada em conformidade com a Resolução CMN n.º 4.893, de 26 de fevereiro de 2021, bem como demais normas do Conselho Monetário Nacional ("CMN"), do Banco Central do Brasil ("BACEN"), da Comissão de Valores Mobiliários ("CVM") e da Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais ("ANBIMA").

2. ABRANGÊNCIA

Esta Política é aplicável para todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança que estejam a serviço da CV DTVM.

Cabe a todos os Colaboradores que utilizam recursos de TI ou acessam informações da CV DTVM cumprirem fielmente esta Política, buscar orientação da Diretoria de Compliance e PLD-FTP e área de TI, em caso de dúvidas relacionadas à segurança da informação e proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, bem como assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas, cumprir as leis e os procedimentos que regulamentam os aspectos de propriedade intelectual e comunicar imediatamente a CV DTVM quando do descumprimento ou violação desta Política.

A presente Política deve ser divulgada a todos os Colaboradores e ficar disponível para consulta sempre que necessário.

3. CONCEITO

As medidas de segurança da informação têm por finalidade preservar o sigilo, a integridade e a disponibilidade das informações da CV DTVM contra uma série de riscos, como fraude, acidentes, roubo, espionagem, perda não-intencional, violação da privacidade e interrupção de serviço e assim minimizar as ameaças aos negócios da Instituição e às disposições desta Política, buscando, principal, mas não exclusivamente, a proteção de informações confidenciais.

Conforme a definição da norma NBR ISO/IEC 17799: 2005, a informação é um ativo que tem valor para a organização e, consequentemente, necessita ser adequadamente protegida. A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

• Confidencialidade: Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;

• Disponibilidade: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária; e

• Integridade: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

É fundamental para a proteção das informações que os Colaboradores estejam corretamente orientados e que adotem a prática segura de utilização dos recursos, devendo também assumir atitudes proativas e engajadas no que diz respeito à segurança das informações e da operação.

As instalações da CV DTVM são protegidas por controles de entrada apropriados para garantir 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 contam com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A presente Política leva em consideração diversos riscos e possibilidades em função do porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela CV DTVM.

A coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Diretoria de Compliance e PLD-FTP, que será a responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

4. DIRETRIZES

Para estabelecer a orientação para a formalização dos procedimentos e orientar as ações e posicionamento dos Colaboradores, as seguintes diretrizes estão formalizadas nesse documento:

(i) As informações (independente do formato que estejam) e os ambientes tecnológicos utilizados pelos Colaboradores são de exclusiva propriedade da CV DTVM, não podendo ser interpretados como de uso pessoal;

(ii) As informações da CV DTVM, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso, exposição indevida ou riscos desnecessários de exposição;

(iii) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;

(iv) Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de uma pessoa ou equipe;

(v) Todos os funcionários, estagiários e prestadores de serviços devem ter ciência de que o uso das informações e dos sistemas de informação são monitorados, e que os registros assim obtidos poderão ser utilizados para detecção de violações desta Política, podendo estas servir de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais;

(vi) O acesso às informações e recursos só deve ser feito se devidamente autorizado pelos responsáveis pela informação. A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades; e

(vii) Os riscos de exposição ou destruição de informações da CV DTVM, devem ser imediatamente reportados diretamente à Diretoria de Compliance e PLD-FTP e a área de TI.

5. IDENTIFICAÇÃO DE RISCOS (RISK ASSESSMENT)

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

- Dados e Informações: as informações confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria CV DTVM, operações e ativos distribuídos, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- Sistemas: informações sobre os sistemas utilizados pela CV DTVM e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da CV DTVM; e

- Governança da Gestão de Risco: a eficácia da gestão de risco pela CV DTVM quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a CV DTVM identificou as seguintes ameaças:

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

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

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

- 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 acima, a CV DTVM 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.

6. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Após a identificação dos riscos, a CV DTVM adota as medidas a seguir descritas para proteger suas informações e sistemas.

- Regra Geral de Conduta

A CV DTVM realiza efetivo controle do acesso a arquivos que contemplem informações confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos da CV DTVM, 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 CV DTVM. 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 CV DTVM 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 Diretoria de Controles, Governança e Relação com o Mercado 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 CV DTVM 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.

A CV DTVM não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

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 as normas internas dispostas acima, os Colaboradores devem se abster de utilizar pen-drivers, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na CV DTVM. É proibida a conexão de equipamentos na rede que não estejam previamente autorizados pela área de informática e pelos administradores.

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 CV DTVM.

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 CV DTVM.

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.

- Classificação de Nível de Confidencialidade

Para assegurar a proteção adequada, é de responsabilidade do diretor de cada área estabelecer a classificação relativa ao nível de confidencialidade das informações sob sua responsabilidade e/ou sob sua guarda segundo os seguintes critérios:

➢ **INFORMAÇÕES PÚBLICAS:** Aquelas destinadas ao público externo. Possuem caráter informativo geral e são direcionadas a clientes ou investidores.

▪ Acesso: Sem restrições para uso operacional;
▪ Transmissão: Sem restrições para uso operacional;
▪ Transporte: Sem restrições após comunicação à área;
▪ Destruição: Após a utilização e trânsito das informações eletrônicas o descarte deverá ser feito com a exclusão dos arquivos e e-mails. Não há restrições para o descarte de documentos físicos.

➢ **INFORMAÇÕES INTERNAS:** São aquelas destinadas ao uso interno. São informações em que a CV DTVM não tem interesse em divulgar externamente, contudo uma eventual exposição não afetaria significativamente a CV DTVM ou seus clientes, investidores e associados.

▪ Acesso: Restrito conforme estrutura de acesso;
▪ Transmissão: Para uso operacional com aprovação do Comitê de Compliance, Governança Corporativa e Riscos;
▪ Transporte: Para uso operacional com aprovação do Comitê de Compliance, Governança Corporativa e Riscos;
▪ Destruição: Após a utilização e trânsito das informações eletrônicas o descarte deverá ser feito com a exclusão dos arquivos e e-mails. O descarte de documentos físicos deve ser feito em fragmentadoras.

➢ **INFORMAÇÕES CONFIDENCIAIS:** Também se destinam a uso interno. Entretanto, diferem das "informações internas" à medida que sua eventual divulgação poderia afetar significativamente os negócios da CV DTVM ou a seus clientes, investidores e associados.

▪ Acesso: Restrito conforme estrutura de acesso. Uso conforme a política de "mesa limpa";
▪ Transmissão: Para uso operacional após aprovação do Comitê de Compliance, Governança Corporativa e Riscos. Envios eletrônicos devem ser criptografados com o arquivo e a senha de acesso enviados separadamente em rota segura. Necessário solicitar a confirmação do recebimento. Os envios de documentos físicos devem ser feitos em envelopes lacrados com a notificação de recebimento.
▪ Transporte: Para uso operacional com aprovação do Comitê de Compliance, Governança Corporativa e Riscos;
▪ Destruição: Após a utilização e trânsito das informações eletrônicas o descarte deverá ser feito com a exclusão dos arquivos e e-mails. O descarte de documentos físicos deve ser feito em fragmentadora.

➢ **INFORMAÇÕES RESTRITAS**: Correspondem a mais alta classificação de segurança para as informações que transitam na CV DTVM. Destina-se às informações cuja divulgação, possivelmente provocaria danos substanciais, constrangimentos ou penalidades a CV DTVM, seus clientes, investidores ou associados. As pessoas designadas para o uso de tais informações, têm a responsabilidade de garantir que elas estejam devidamente protegidas e armazenadas de forma segura quando não estiverem em uso.

▪ Acesso: Restrito conforme estrutura de acesso. Arquivos com chaves de criptografia e uso conforme a política de "mesa limpa";
▪ Transmissão: Realizados somente por membros do Comitê de Compliance, Governança Corporativa e Riscos. Envios eletrônicos devem ser criptografados com o arquivo e a senha de acesso enviados separadamente em rota segura. Necessário solicitar a confirmação do recebimento. Os envios de documentos físicos devem ser feitos em envelopes lacrados com a notificação de recebimento.
▪ Transporte: Restrito somente ao Comitê de Compliance, Governança Corporativa e Riscos. Armazenamento criptografado;
▪ Destruição: Após a utilização e trânsito das informações eletrônicas o descarte deverá ser feito com a exclusão dos arquivos e e-mails de forma que não seja possível sua recuperação. O descarte de documentos físicos deve ser feito em fragmentadora.

As responsabilidades de cada um dos envolvidos quanto à segurança das informações, e suas respectivas classificações, devem ser amplamente divulgadas a todos Colaboradores que utilizam ou tem acesso às informações, que devem entender e assegurar esta diretriz.

- Acesso Escalonado do Sistema

O acesso como “administrador” ao sistema operacional do computador é limitado aos usuários aprovados pelo Comitê de Compliance, Governança Corporativa e Riscos e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

A CV DTVM, 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 DTVM, necessária ao exercício de suas atividades.

A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas a partir dos acessos utilizando sua identificação.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da CV DTVM 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 utilizadas nos computadores e rede deverão seguir os critérios abaixo:

(i) Período de expiração – a validade da senha será de no máximo 90 dias, sendo o usuário obrigado a renovar a senha após esse período;

(ii) Composição da senha - obrigatoriedade de no mínimo 8 caracteres, sendo que deve ser atendida pelo menos 3 condições de 4 apresentadas (Caixa alta, Caixa baixa, números e caracteres especiais);

(iii) Histórico de senha – a senha não pode ser igual as últimas 10 senhas utilizadas anteriormente, se aplicável;

(iv) Bloqueio de senha – a senha(conta) será bloqueada caso seja digitada de forma errada por 5 tentativas e só poderá ser desbloqueada pelo administrador;

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 Instituição, 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, bem como 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 e PLD-FTP.

- Acesso Remoto/VPN

A CV DTVM permite o acesso remoto via VPN para os Colaboradores, de acordo com a seguinte regra: a todos os Colaboradores, conforme requisição por estes e autorização pela Diretoria de Compliance e PLD-FTP e Política interna, no que se refere ao acesso ao e-mail, à rede e diretórios internos.

Ademais, os Colaboradores autorizados serão instruídos a (i) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (ii) relatar a Diretoria de Compliance e PLD-FTP e área de TI, qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Instituição e que ocorram durante o trabalho remoto, e (iii) não armazenar informações confidenciais ou sensíveis em dispositivos pessoais.

- Controle de Acesso

O acesso de pessoas estranhas as áreas restritas somente são permitidas com a autorização expressa de Colaboradores autorizados pelos administradores.

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 CV DTVM monitora a utilização de tais meios.

- *Firewall, Software*, Varreduras e *Backup.*

A Instituição utiliza um *hardware* de *firewall* projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. A Diretoria de Compliance e PLD-FTP é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

A CV DTVM 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*). São conduzidas varreduras, diárias para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Instituição.

A CV DTVM mantém e testa regularmente medidas de backup consideradas apropriadas pela Diretoria de Compliance e PLD-FTP e área de TI. As informações do Grupo CVPAR são atualmente objeto de backup **diário** com o uso de computação na nuvem.

6.1. Monitoramento e Testes

A Instituição 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, **semestral**:

(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 para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação; 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.

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

6.2. Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da CV DTVM (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer informações confidenciais, mesmo que de forma involuntária, deverá ser informado a Diretoria de Compliance e PLD-FTP que solicitará uma reunião do Comitê de Compliance, Governança Corporativa e Riscos prontamente. Essa comunicação deve ser feita por telefone e formalizada por e-mail. Os demais incidentes devem ser reportados em até 4 horas após a percepção da falha. O Comitê de Compliance, Governança Corporativa e Riscos determinará quais membros da administração, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Comitê de Compliance, Governança Corporativa e Riscos determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

- Procedimentos de Resposta

A Diretoria de Compliance e PLD-FTP em conjunto com a área de TI responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Instituição 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;

(v) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(vi) Determinação dos papéis e responsabilidades do pessoal apropriado;

(vii) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(viii) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

(ix) 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 gestão do Grupo CVPAR, a fim de garantir a ampla disseminação e tratamento equânime da informação confidencial); e

(x) Determinação do responsável (ou seja, a CV DTVM ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Comitê de Compliance, Governança Corporativa e Riscos, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

6.3. Arquivamento de Informações

De acordo com o disposto nesta Política, 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.

7. 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 a CV DTVM, 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 distribuição, em qualquer formato, são e permanecerão sendo propriedade exclusiva da CV DTVM, 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, devendo todos os documentos permanecerem em poder e sob a custódia da CV DTVM, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento, salvo se autorizado expressamente pelo e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto a CV DTVM, o Colaborador deverá assinar declaração nos termos do **Anexo I** 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 CV DTVM, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais

documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento, exceto se aprovado expressamente pela CV DTVM.

8. TREINAMENTO

A Diretoria de Compliance e PLD-FTP organizará treinamento **anual** dos Colaboradores com relação às regras e procedimentos acima. Adicionalmente, orientações técnicas para a melhor operação dos sistemas e de compliance deverão ser abordadas na contratação de novos profissionais assim como nas atualizações a serem feitas de forma contínua.

9. REVISÃO DA POLÍTICA

A Diretoria de Compliance e PLD-FTP realizará uma revisão desta Política anualmente, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais, devendo levar os resultados ao Comitê de Compliance, Governança Corporativa e Riscos que decidirá sobre a alteração desta Política caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência, sendo que qualquer alteração deverá ser amplamente divulgada a todas as áreas e Colaboradores pela Diretoria de Compliance e PLD-FTP.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da CV DTVM e acontecimentos regulatórios relevantes.

Histórico das atualizações			
Data	Versão	Responsável	Descrição
Maio de 2023	1ª	Diretor de Controles, Governança e Relação com o Mercado	Criação do Documento
Novembro de 2024	2º e Atual	Diretor de Controles, Governança e Relação com o Mercado	Atualização de informações restritas.

ANEXO I
TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o nº _____ ("Colaborador"), DECLARO para os devidos fins:

(i) que a disponibilização pelo Colaborador à **CV INVESTIMENTOS DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA.** ("CV DTVM"), nesta data, dos documentos listados abaixo ("Documentos"), bem como sua futura utilização pela CV DTVM, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e

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

Para os devidos fins, o Colaborador atesta que os Documentos foram copiados e ficarão com a CV DTVM e cujo conteúdo é idêntico ao Documento disponibilizado pelo Colaborador.

Os Documentos fazem parte integrante do presente termo, para todos os fins e efeitos de direito. A lista dos Documentos se encontra no Apêndice ao presente termo.

[•], [•] de [•] de [•].

_____
[COLABORADOR]

➔ Apêndice

Lista dos Arquivos
