Data da Atualização	Responsável	Versão
Abril de 2026	Diretor de Compliance, Risco e PLD/FTP	6ª

POLÍTICA SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS

Data da Atualização	Responsável	Versão
Abril de 2026	Diretor de Compliance, Risco e PLD/FTP	6ª

I. OBJETIVO E ABRANGÊNCIA

- *Sumário*

A **CVPAR INVESTIMENTOS LTDA.** ("Gestora") desenvolveu a presente Política de Regras, Procedimentos e Descrição dos Controles Internos ("Política") observando a regulamentação da Comissão de Valores Mobiliários ("CVM") e autorregulação da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de forma a estabelecer diretrizes e princípios que orientem o comportamento ético e profissional dos administradores, empregados e colaboradores da Gestora ("Colaboradores"), incluindo as suas condutas internas no âmbito do exercício de suas atividades profissionais, sempre pautadas com base no compliance interno.

Dessa forma, esta política foi elaborada observando as seguintes principais regras, normas e orientações regulatórias e autorregulatórias:

- Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21");
- Código da ANBIMA de Administração e Gestão de Recursos de Terceiros ("Código de AGRT") e demais disposições acessórias a este Código;
- Código da ANBIMA de Ética ("Código de Ética") e demais disposições acessórias a este Código;
- Código ANBIMA de Certificação Continuada ("Código de Certificação"); e
- Demais documentos divulgados pela regulação e autorregulação que forem aplicáveis às atividades da Gestora.

- *Declaração de Recebimento e Compromisso*

Esta política integra-se às diretrizes que regem a relação entre a Gestora e os seus respectivos Colaboradores. Ao subscreverem a Declaração de Recebimento e Compromisso, conforme o Anexo I desta Política, os Colaboradores manifestam expressamente a aceitação das normas, princípios, conceitos e valores aqui delineados.

É incumbência de todos os Colaboradores assegurar um entendimento preciso das leis e normas aplicáveis à Gestora, assim como do conteúdo integral desta Política.

Ao receberem esta Política, os Colaboradores formalizam sua adesão por meio da Declaração de Recebimento e Compromisso. Por meio deste documento, reconhecem e confirmam ciência e concordância com os termos desta Política, bem como as normas, princípios, conceitos e valores nele contidos. Comprometem-se a zelar pela aplicação das normas de compliance e pelos princípios aqui apresentados. Periodicamente, poderá ser requerido dos Colaboradores a assinatura de novas Declarações de Recebimento e Compromisso para reforçar o entendimento e a concordância com os termos desta Política.

Data da Atualização	Responsável	Versão
Abril de 2026	Diretor de Compliance, Risco e PLD/FTP	6ª

A não conformidade, suspeita ou indício de violação de qualquer norma, princípio, conceito ou valor estabelecido nesta Política ou de outras normas aplicáveis às atividades da Gestora, deverá ser comunicada ao Diretor de Compliance, Risco e PLD/FTP, conforme definido abaixo, seguindo os procedimentos estabelecidos nesta Política. Caberá ao Diretor de Compliance, Risco e PLD/FTP aplicar as sanções decorrentes desses desvios, de acordo com esta Política, garantindo ao Colaborador direito de defesa.

É dever de todo colaborador informar ao Diretor de Compliance, Risco e PLD/FTP sobre violações ou possíveis violações dos princípios e normas aqui estabelecidos, visando preservar os interesses dos clientes da Gestora e zelar pela reputação da sociedade. Se a violação ou suspeita de violação envolver o próprio Diretor de Compliance, Risco e PLD/FTP, o Colaborador deverá comunicar diretamente aos demais administradores da Gestora.

Data da Atualização	Responsável	Versão
Abril de 2026	Diretor de Compliance, Risco e PLD/FTP	6ª

SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS

O propósito das medidas adotadas referentes a segurança da informação é de reduzir as ameaças aos interesses comerciais da Gestora, alinhando-se às diretrizes deste Manual e, principalmente, visando à proteção das Informações Confidenciais. Para garantir a segurança dos Colaboradores e preservar o sigilo, integridade e disponibilidade da informação, são implementados controles de acesso apropriados nas instalações da Gestora, conforme a seguir expostos.

A disposição dos equipamentos de rede exige que estes sejam armazenados em uma sala com acesso restrito. As estações de trabalho são fixas, equipadas com computadores seguros, e é obrigatório trancar as sessões abertas quando não estão sob supervisão do Colaborador responsável pelo respectivo computador. A política de segurança cibernética e de proteção de dados leva em conta vários riscos e cenários, considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades da Gestora.

A responsabilidade direta pela coordenação das iniciativas relacionadas à esta política é atribuída ao Diretor de Compliance, Risco e PLD/FTP. Este diretor não apenas supervisionará a implementação dessas medidas, mas também será encarregado de revisá-las, conduzir testes e proporcionar treinamento aos Colaboradores, conforme detalhado abaixo.

É terminantemente proibido usar e/ou instalar softwares ou aplicativos sem licença ou que não tenham sido adquiridos ou previamente homologados/autorizados pela Gestora. É proibido utilizar o *e-mail* institucional para fins pessoais.

- *Identificação de Riscos (risk assessment)*

A Gestora identificou que os riscos indicados abaixo necessitam de maior resguardo, incluindo, mas não se limitando a:

a. Sistemas: Isso inclui dados sobre os sistemas empregados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, juntamente com suas possíveis ameaças e vulnerabilidades.

b. Governança da Gestão de Risco: Diz respeito à efetividade da gestão de riscos realizada pela Gestora no que tange às ameaças identificadas.

c. Dados e Informações: Isso abrange as Informações Confidenciais, que englobam dados relativos a investidores, clientes, Colaboradores e à própria Gestora, além de informações sobre as operações realizadas.

d. Processos e Controles: Aqui se enquadram os processos e controles internos que integram a rotina das diversas áreas de negócio da Gestora.

Não obstante, conforme o Guia de Cibersegurança divulgado pela ANBIMA, destacam-se abaixo os principais ataques cibernéticos que a Gestora poderá enfrentar:

a. *Malware* – softwares desenvolvidos para corromper computadores e redes (por exemplo: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

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

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

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

- *Ações de Prevenção e Proteção*

A Gestora desenvolveu e estabeleceu um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, que busca impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles internos adequados e robustos.

Objeto	Conduta
Controlar o acesso adequado aos ativos da Gestora	Os Colaboradores apenas irão conseguir realizar o acesso as suas ferramentas de trabalho através de desktop ou notebook, o qual deverá conter uma senha pessoal e intransferível.
Definição de Senhas	Os Colaboradores deverão trocar as suas senhas a cada 90 (noventa) dias. Nesse sentido, os Colaboradores receberão uma notificação quando o prazo para esta ação estiver se aproximando.
Limitação de Acesso aos Colaboradores	Cada Colaborador, quando de sua entrada na Gestora, receberá uma permissão específica para entrar nas pastas e diretórios de rede aplicáveis à sua atividade. Caso seja necessário acessar um documento e/ou pasta que não possua permissão, deverá solicitar o acesso ao Diretor de Compliance, Risco e PLD/FTP.

Ativos da Gestora	Os ativos tecnológicos da Gestora estão instalados em um ambiente fechado em que apenas Colaboradores autorizados pelo Diretor de Compliance, Risco e PLD/FTP estão autorizados para entrar. Adicionalmente, os Colaboradores da Gestora poderão desempenhar as suas tarefas através de *homeoffice*, sendo que, para tanto, serão instruídos pelo Diretor de Compliance, Risco e PLD/FTP de como realizarem.
Restrição de acesso físico às áreas com informações críticas/sensíveis	Para que os Colaboradores possam acessar o ambiente físico da Gestora pela primeira vez, será necessário realizarem de forma prévia um acesso, em que serão coletadas as suas informações pessoais registrada a sua impressão digital no sistema de controle de acesso. Para as demais entradas no espaço físico da Gestora, será suficiente apenas a autenticação biométrica por meio da impressão digital.
Backup	A Gestora conta atualmente com um *backup* diário, em que todas as informações disponíveis para acesso no servidor da sociedade ficam disponíveis na nuvem.
Firewall	*Hardwares* e *firewall* impedem acessos não autorizados e protegem contra invasões maliciosas. O Diretor de Compliance, Risco e PLD/FTP define o uso adequado dos *firewalls*, garantindo a segurança do perímetro da rede.
Proteção contra *Malware*	Softwares antivírus atualizados detectam, previnem e eliminam programas maliciosos (vírus, *ransomware*, *Worms* e *spyware*) nos dispositivos da Gestora. Varreduras constantes identificam e removem qualquer programa que obtenha acesso indevido à rede.

- <u>*Monitoramento e Testes*</u>

Data da Atualização	Responsável	Versão
Abril de 2026	Diretor de Compliance, Risco e PLD/FTP	6ª

O Diretor de Compliance, Risco e PLD/FTP realiza, no mínimo **anualmente** e sempre que julgar necessário, o monitoramento por amostragem do acesso dos Colaboradores a:

- Sites, blogs, fotologs, *webmails*; e
- *E-mails* enviados e recebidos.

Também por amostragem, verifica as informações de acesso a:

- Espaço do escritório; e
- *Desktops*, pastas e sistemas utilizados.

O objetivo é avaliar a aderência às regras de restrição de acesso e escalonamento. O Diretor de Compliance, Risco e PLD/FTP pode adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos previstos, avaliando seu cumprimento e eficácia.

- *Plano de Identificação e Resposta a Incidentes: Detalhes e Fundamentação*

A segurança da informação é fundamental para proteger os ativos da Gestora contra ameaças cibernéticas. Um plano de identificação e resposta a incidentes é essencial para minimizar o impacto de eventos de segurança e garantir a continuidade dos negócios.

Este plano abrangente define as etapas a serem tomadas para identificar, classificar e responder a incidentes de segurança de forma eficaz e eficiente. Ele envolve a participação de diferentes áreas da Gestora, incluindo a equipe de tecnologia da informação que auxilia a Gestora e a Área de Compliance, que em conjunto são a "Equipe de Contingência".

O Colaborador deverá imediatamente reportar qualquer ameaça e, caso tenha dúvida, solicite esclarecimentos imediatos ao Diretor de Compliance, Risco e PLD/FTP. A agilidade é fundamental para minimizar eventuais ameaças e por este motivo é importante que os Colaboradores reportem com a máxima brevidade possível.

  - *Envolvimento e Responsabilidades:*

A Equipe de Contingência é composta por especialistas em segurança da informação e pela Área de Compliance da Gestora. Essa equipe multidisciplinar garante uma visão holística dos incidentes e permite uma tomada de decisões rápida e eficaz quando configurada alguma situação de contingência.

Colaboradores-chave em cada área da Gestora são identificados e treinados para assumirem responsabilidades específicas em caso de incidente. Neste caso é o Diretor de Compliance, Risco e PLD/FTP e o responsável pela área de tecnologia da informação da Gestora.

Contatos externos com autoridades, empresas de segurança cibernética e outros parceiros

relevantes são estabelecidos para garantir suporte especializado em casos de incidentes complexos e deverão ser avaliados conforme a cada caso.

- *Processo de Resposta:*

O monitoramento contínuo dos sistemas e da rede detecta atividades anormais. Ferramentas e técnicas avançadas de detecção, como análise de anomalias e correlação de eventos de segurança, identificam potenciais incidentes.

Uma investigação completa é realizada utilizando ferramentas tecnológicas e de resposta a incidentes para determinar a causa, o escopo e o impacto do incidente.

A equipe de resposta a incidentes e os colaboradores-chave são notificados imediatamente, utilizando canais de comunicação adequados à severidade do incidente.

- *Classificação:*

A severidade do incidente é classificada com base em critérios predefinidos, como impacto nos negócios, risco de perda de dados e potencial de escalada. Essa classificação determina o nível de resposta necessário.

- *Resposta:*

A resposta ao incidente é direcionada para conter o problema, minimizar o impacto nos negócios e restaurar os sistemas e dados afetados.

Medidas de contenção, como isolamento de sistemas infectados, podem ser necessárias para evitar a propagação do incidente.

A investigação completa determina a causa do incidente e identifica as medidas corretivas necessárias para evitar sua reincidência.

A recuperação dos sistemas e dados afetados é realizada de forma segura e eficiente, utilizando backups e outras soluções de recuperação de desastres.

- *Documentação e Aprendizagem:*

Todas as ações tomadas durante o incidente são documentadas para fins de auditoria, investigação e aprimoramento do plano de resposta.

Lições aprendidas em incidentes anteriores são utilizadas para revisar e atualizar o plano de resposta a incidentes regularmente.

- *Arquivamento de Informações*

Conforme estabelecido neste Manual, os Colaboradores assumem a responsabilidade de manter arquivados, pelo período legal aplicável, todos os dados, documentos e extratos que se mostrarem necessários para o pleno atendimento de auditorias ou investigações relacionadas a:

- Possíveis investimentos que levantem suspeitas de irregularidades; e
- Clientes sob investigação por práticas de corrupção ou lavagem de dinheiro, em estrita observância às normas e leis em vigor.

➢ *Propriedade Intelectual*

A Gestora reconhece a importância de proteger sua propriedade intelectual e as informações confidenciais. Para garantir a ética, a transparência e a segurança dos seus ativos, a Gestora implementa uma política rigorosa que se aplica a todos os Colaboradores. No ingresso dos Colaboradores na Gestora, eles deverão preencher o Termo de Propriedade Intelectual, cujo modelo encontra-se no Anexo III.

o *Documentos e Arquivos:*

Todos os documentos e arquivos relacionados ao trabalho na Gestora, incluindo minutas de contrato, *e-mails*, planilhas e modelos de avaliação, são de propriedade exclusiva da Gestora.

O Colaborador não pode utilizar esses documentos para fins pessoais, mesmo após o desligamento da Gestora. Desta forma, a Gestora tem a posse e a guarda de todos os documentos.

o *Documentos do Colaborador:*

Caso o Colaborador forneça à Gestora documentos, planilhas ou modelos de avaliação para o seu trabalho, ele deverá assinar uma declaração confirmando que: (i) a utilização desses documentos não viola nenhum contrato ou acordo de confidencialidade previamente estabelecido; e (ii) a Gestora será a única proprietária de quaisquer alterações feitas nesses documentos.

O Colaborador não poderá usar os documentos alterados após sair da Gestora, exceto com autorização da própria Gestora.

o *Importância da Propriedade Intelectual e Confidencialidade:*

Protegem os ativos e documentos da Gestora contra uso indevido e concorrência desleal, bem como evitam o vazamento de informações confidenciais que podem prejudicar a Gestora, seus clientes e parceiros e garantem a ética e a transparência nas relações da Gestora com todos os públicos, incluindo os seus Colaboradores e clientes.

Data da Atualização	Responsável	Versão
Abril de 2026	Diretor de Compliance, Risco e PLD/FTP	6ª

- *Compromisso do Colaborador:*

Ao se integrar à Gestora, o Colaborador se compromete a proteger a propriedade intelectual e a confidencialidade da Gestora.

O Colaborador deve usar os documentos e arquivos da sociedade de forma responsável e ética, apenas para o desempenho de suas atividades profissionais. Nesse sentido, ao se desligar da sociedade, o Colaborador deve devolver todos os documentos e arquivos da Gestora em seu poder, inclusive aqueles que tenha desenvolvido no âmbito de suas tarefas profissionais junto à Gestora.

A Gestora acredita que a proteção da propriedade intelectual e da confidencialidade é essencial para o sucesso da empresa e para a construção de um ambiente de trabalho ético e transparente.

- *Revisão da Política*

Esta Política de Segurança Cibernética e Proteção de Dados deverá ser revisada pelo Diretor de Compliance, Risco e PLD/FTP em periodicidade inferior a 24 (vinte e quatro) meses, e sempre que identificada a necessidade de atualização em prazo inferior, decorrente de alterações regulatórias e/ou autorregulatórias, o referido Diretor o fará.

ANEXO I
DECLARAÇÃO DE CIÊNCIA E CONCORDÂNCIA

Eu, [Nome Completo do Colaborador], CPF [Número do CPF do Colaborador], RG [Número do RG do Colaborador], colaborador da **CVPAR INVESTIMENTOS LTDA.** ("Gestora"), declaro para os devidos fins e efeitos, que recebi uma cópia do Manual de Regras, Procedimentos e Descrição dos Controles Internos da Gestora ("Manual").

Declaro ainda que li, compreendi e estou ciente das obrigações, responsabilidades e diretrizes estabelecidas no referido Manual, incluindo, mas não se limitando a questões relacionadas à segurança da informação, política de anticorrupção, deveres e condutas, dentre outros tópicos relevantes.

Comprometo-me a adotar uma conduta pautada pelos valores éticos e morais estabelecidos no Manual, zelando pela integridade da Gestora, de seus clientes, parceiros e demais partes interessadas.

Declaro, por fim, que estou ciente de que o não cumprimento das disposições contidas no Manual poderá acarretar medidas disciplinares conforme previsto no Manual, sem prejuízo das punições previstas na legislação vigente.

Local e Data: [Local e Data de Assinatura da Declaração]

Assinatura: _____(Nome do Colaborador)

ANEXO II
TERMO DE CONFIDENCIALIDADE

Pelo presente instrumento, Eu, [Nome Completo do Colaborador], CPF [Número do CPF do Colaborador], RG [Número do RG do Colaborador], colaborador da **CVPAR INVESTIMENTOS LTDA.** ("Gestora") e a própria Gestora resolvem celebrar o presente termo de confidencialidade ("Termo"), que se regerá pelas cláusulas abaixo:

Cláusula 1º. O Colaborador se compromete a manter em sigilo absoluto todas as informações confidenciais, de qualquer natureza, a que tenha acesso em razão de seu vínculo com a Gestora, incluindo, mas não se limitando a:

(i) Informações financeiras e comerciais da Gestora e de seus clientes;
(ii) Dados de clientes, parceiros e fornecedores;
(iii) Estratégias de negócios e planos de marketing;
(iv) Processos e procedimentos internos da Gestora; e
(v) Qualquer outra informação que seja considerada confidencial pela Gestora.

Cláusula 2º. Do Uso das Informações Confidenciais

O Colaborador se compromete a utilizar as informações confidenciais única e exclusivamente para o desempenho de suas funções na Gestora, sendo vedado:

(i) Divulgar as informações confidenciais a terceiros, inclusive familiares e amigos;
(ii) Utilizar as informações confidenciais para benefício próprio ou de terceiros;
(iii) Reproduzir, copiar ou transmitir as informações confidenciais por qualquer meio; e
(iv) Armazenar as informações confidenciais em local não seguro.

Cláusula 3º. Das Exceções à Confidencialidade

O Colaborador poderá divulgar as informações confidenciais quando:

(i) For obrigado por lei ou ordem judicial;
(ii) For autorizado por escrito pela Gestora;
(iii) For necessário para a defesa de seus direitos em processo judicial ou administrativo.

Cláusula 4º. Da Vigência

O presente Termo de Confidencialidade terá vigência durante todo o período em que o Colaborador estiver vinculado à Gestora, e por prazo de 5 (cinco) anos após o seu desligamento.

Cláusula 5º. Das Sanções

O descumprimento de qualquer das cláusulas do presente Termo de Confidencialidade sujeitará o Colaborador às seguintes sanções:

(i) Rescisão do contrato de trabalho, por justa causa;
(ii) Pagamento de multa equivalente a 6 (seis) vezes a última remuneração mensal recebida; e
(iii) Responsabilidade civil e criminal pelos danos causados à Gestora.

Cláusula 6º. Disposições Gerais

O presente Termo de Confidencialidade é firmado em duas vias de igual teor e forma, para que produza os seus jurídicos e legais efeitos.

O Colaborador declara que foi expressamente informado de que o e-mail institucional é de propriedade da empresa e que poderá ser monitorado a qualquer momento, inclusive por meio do acesso e leitura às mensagens enviadas e recebidas. É proibido utilizar o e-mail institucional para fins pessoais.

As partes elegem o Foro da Comarca da Capital do Estado em que se situa a sede da Gestora para dirimir qualquer litígio que possa surgir em decorrência do presente instrumento.

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.

Local e Data: [Local e Data de Assinatura da Declaração]

Assinatura: _____
(Nome do Colaborador)

Assinatura: _____
CVPAR INVESTIMENTOS LTDA.

Testemunhas:

1._____ 2._____

Nome: Nome:
CPF: CPF: