Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

MANUAL DE REGRAS, PROCEDIMENTOS E DESCRIÇÃO DOS CONTROLES INTERNOS

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

I. OBJETIVO E ABRANGÊNCIA

- *Sumário*

A **CVPAR HIERON INVESTIMENTOS LTDA.** ("Gestora") desenvolveu o presente Manual de Regras, Procedimentos e Descrição dos Controles Internos ("Manual") 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, este Manual foi elaborado 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");
- Código ANBIMA de Distribuição de Produtos de Investimento ("Código de Distribuição"), conforme aplicável; e
- Demais documentos divulgados pela regulação e autorregulação que forem aplicáveis às atividades da Gestora.

- *Declaração de Recebimento e Compromisso*

Este Manual 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 deste Manual, 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 deste Manual.

Ao receberem este Manual, 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 deste Manual, 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

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

Compromisso para reforçar o entendimento e a concordância com os termos deste Manual.

A não conformidade, suspeita ou indício de violação de qualquer norma, princípio, conceito ou valor estabelecido neste Manual, 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 neste Manual. Caberá ao Diretor de Compliance, Risco e PLD/FTP aplicar as sanções decorrentes desses desvios, de acordo com este Manual, 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
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

POLÍTICA DE COMPLIANCE

I. INTRODUÇÃO

- *Obrigações Internas da Área de Compliance*

A responsabilidade pela coordenação das atividades relacionadas a este Manual é atribuída ao diretor da Gestora designado em seu Contrato Social, como o diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Gestora, denominado "Diretor de Compliance, Risco e PLD/FTP ", conforme estipulado na Resolução CVM nº 21.

Incluem-se dentre as tarefas do Diretor de Compliance, Risco e PLD/FTP, mas não se limitam a:

(i) Acompanhar as políticas descritas neste Manual;

(ii) Encaminhar pedidos de autorização, orientação, esclarecimento ou relatar ocorrências, suspeitas ou indícios de práticas contrárias às disposições deste Manual e demais normas aplicáveis à atividade da Gestora para análise dos administradores da sociedade;

(iii) Identificar possíveis condutas em desacordo com este Manual;

(iv) Centralizar informações e realizar revisões periódicas dos processos de compliance, especialmente em casos de alterações nas políticas vigentes ou aumento no número de colaboradores;

(v) Assessorar a gestão de negócios no entendimento, interpretação e impacto da legislação, monitorando as melhores práticas e analisando periodicamente as normas emitidas por órgãos competentes como a CVM e outros organismos similares;

(vi) Elaborar um relatório **anual** listando as operações suspeitas comunicadas às autoridades competentes, nos termos da regulamentação em vigor;

(vii) Submeter aos órgãos de administração da Gestora, até o último dia útil de **abril** de cada ano, um relatório referente ao ano civil anterior, contendo: (a) conclusões dos exames realizados; (b) recomendações sobre eventuais deficiências, com cronogramas de saneamento, quando necessário; e (c) a manifestação do diretor responsável pelas atividades de administração de carteiras de valores mobiliários e distribuição de fundos próprios a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las;

(viii) Promover a ampla divulgação e aplicação dos preceitos éticos nas atividades de todos os Colaboradores, incluindo treinamentos periódicos conforme previsto neste Manual;

(ix) Avaliar todos os casos relacionados ao potencial descumprimento dos preceitos éticos e de compliance estabelecidos neste Manual ou em outros documentos mencionados, além de analisar situações não previstas;

(x) Garantir o sigilo de informantes de delitos ou infrações, mesmo quando não

solicitado, exceto em casos que demandem testemunho judicial;

(xi) Solicitar, sempre que necessário, o apoio da auditoria interna ou externa ou outros assessores profissionais para análise de questões específicas;

(xii) Aplicar eventuais sanções aos Colaboradores; e

(xiii) Analisar situações que cheguem ao seu conhecimento e que possam caracterizar "conflitos de interesse" pessoais e profissionais.

Qualquer Colaborador ciente de informações ou situações em curso que possam afetar os interesses da Gestora, gerar conflitos e/ou contrariar os termos deste Manual deve informar o Diretor de Compliance, Risco e PLD/FTP para adoção das medidas apropriadas.

O Diretor de Compliance, Risco e PLD/FTP pode contar com outros Colaboradores para atividades e rotinas de compliance, com atribuições específicas determinadas conforme a necessidade da Gestora e a senioridade do Colaborador.

Por fim, a Gestora contará em sua estrutura interna com um Comitê de Risco e Compliance, nos termos de seu Regimento Interno, o qual possuirá, dentre as suas atribuições, avaliar e discutir sobre eventuais falhas e oportunidades de aperfeiçoamento nos controles internos da Gestora.

- *Esclarecimentos e formas de contato com o Diretor de Compliance, Risco e PLD/FTP*

Em situações de incerteza sobre os temas abordados neste Manual, é essencial procurar imediatamente a orientação do Diretor de Compliance, Risco e PLD/FTP para receber o suporte adequado.

Mesmo diante de suspeitas mínimas de possíveis conflitos ou de ações que possam prejudicar os interesses da Gestora, os Colaboradores devem seguir a mesma orientação. Essa abordagem é vista como a forma mais transparente e objetiva de consolidar os valores da cultura empresarial da Gestora e reforçar seus princípios éticos.

Dentro do escopo deste Manual, qualquer solicitação que exija autorização, orientação ou esclarecimento direto do Diretor de Compliance, Risco e PLD/FTP, assim como qualquer ocorrência, suspeita ou indício de prática por parte de qualquer colaborador que não esteja em conformidade com as disposições deste Manual e outras normas aplicáveis às atividades da Gestora, deve ser comunicada pela pessoa que necessita da autorização, orientação ou esclarecimento, ou que tome conhecimento da ocorrência ou suspeite ou possua indícios de práticas em desacordo com as regras aplicáveis, ao Diretor de Compliance, Risco e PLD/FTP, exclusivamente por meio de e-mail.

- *Procedimentos internos de supervisão periódica*

Em caso de violação, suspeita ou indício de não conformidade com as diretrizes estabelecidas neste Manual ou aplicáveis às atividades da Gestora, que cheguem ao

conhecimento do Diretor de Compliance, Risco e PLD/FTP, seguindo os procedimentos delineados neste Manual, o Diretor em questão poderá fazer o uso dos registros e sistemas de monitoramento eletrônico mencionados neste Manual para avaliar a conduta dos Colaboradores envolvidos.

A totalidade do conteúdo disponível *online* estará sujeita à verificação pelo Diretor de Compliance, Risco e PLD/FTP, caso seja necessário, inclusive, arquivos pessoais salvos em cada computador serão examinados, conforme avaliação do Diretor de Compliance, Risco e PLD/FTP. Da mesma forma, as comunicações por *e-mail* dos Colaboradores serão registradas e, quando necessário, verificadas e acessadas, sem que isso seja considerado uma invasão de privacidade, dado que se tratam de ferramentas de trabalho disponibilizadas pela Gestora. Toda a comunicação com clientes, autoridades governamentais, colaboradores e fornecedores deverá ser realizada obrigatoriamente e de forma exclusiva pelo *e-mail* institucional disponibilizado pela Gestora, sendo vedado o registro de autorizações ou operações por aplicativos de mensagens. É terminantemente proibido utilizar *e-mails* pessoais ou aplicativos pessoais na comunicação institucional, inclusive com clientes.

As informações obtidas desses sistemas poderão ser utilizadas pelo Diretor de Compliance, Risco e PLD/FTP para tomar decisões a respeito de possíveis penalidades aos Colaboradores envolvidos, conforme as disposições deste Manual e/ ou comunicadas às Autoridades Governamentais, conforme o caso.

Adicionalmente, o Diretor de Compliance, Risco e PLD/FTP deverá realizar verificações regulares nos níveis de controles internos e conformidade em todas as áreas da Gestora, buscando tomar medidas para esclarecer e corrigir possíveis não conformidades. Ele também revisará os controles descritos neste Manual, bem como em outras políticas da Gestora, sugerindo a implementação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções.

Além dos procedimentos de supervisão periódica, o Diretor de Compliance, Risco e PLD/FTP poderá realizar inspeções nas ferramentas de trabalho a qualquer momento, conforme julgar apropriado e necessário, em relação a qualquer Colaborador.

- *Independência na Atuação*

Os membros que atuarem nas funções de compliance comporão a Área de Compliance, que estará sob a supervisão do Diretor de Compliance, Risco e PLD/FTP. É importante destacar que a Área de Compliance desempenha suas atribuições de maneira totalmente autônoma em relação às demais áreas da Gestora e terá a capacidade de exercer sua autoridade e poderes sobre qualquer Colaborador.

- *Dever de Reportar*

O Colaborador que tomar ciência ou suspeitar de qualquer ato em desacordo com as disposições deste Manual deve, de imediato, informar tal ocorrência ao Diretor de Compliance, Risco e PLD/FTP. Nenhum Colaborador enfrentará represálias por denunciar, de maneira honesta, violações ou potenciais violações a este Manual. Ademais, todas as notificações e investigações serão tratadas com confidencialidade, na medida do possível nessas circunstâncias. No entanto, o Colaborador que deixar de cumprir essa obrigação poderá estar sujeito não apenas a medidas disciplinares, mas também à demissão por justa causa, de acordo com o regime jurídico vigente.

- *Sanções ("Enforcement")*

O Diretor de Compliance, Risco e PLD/FTP é responsável pela aplicação de eventuais sanções decorrentes do não cumprimento dos princípios deste Manual. Tais sanções podem incluir advertência, suspensão, desligamento ou exclusão por justa causa, se o Colaborador for sócio da Gestora. Para Colaboradores que sejam empregados, a demissão por justa causa é uma opção, conforme o artigo 482 da CLT, sem prejuízo do direito de a Gestora buscar indenização pelos prejuízos, perdas, danos e/ou lucros cessantes por meio de medidas legais cabíveis.

A Gestora não assume a responsabilidade por Colaboradores que violem a lei ou cometam infrações em suas funções. Se a Gestora for responsabilizada ou sofrer prejuízos devido a ações de seus Colaboradores, reserva-se o direito de regresso contra os responsáveis.

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

CONFIDENCIALIDADE NA GESTORA

- *Sigilo e Conduta*

As normativas presentes neste Capítulo são destinadas aos Colaboradores que, por meio de suas incumbências na Gestora, possam ter ou venham a ter acesso a informações confidenciais, reservadas ou privilegiadas, abrangendo aspectos financeiros, técnicos, comerciais, estratégicos, negociais, econômicos, entre outros.

É necessário que todos os Colaboradores leiam e compreendam as disposições contidas neste Manual, sendo também necessário assinar a Declaração de Confidencialidade, conforme modelo apresentado no Anexo II.

Nesse sentido, com base na Declaração de Confidencialidade, é estritamente proibido divulgar qualquer Informação Confidencial, conforme definido a seguir, para fora da Gestora. Qualquer divulgação, seja no âmbito pessoal ou profissional, que não esteja em conformidade com as normas legais, está expressamente vetada.

São consideradas como Informações Confidenciais, aquelas que não possam ser tornadas públicas, incluindo, mas não se limitando a:

(i) Portfólio de Ativos: Composição detalhada do portfólio de ativos, incluindo tipos de títulos, valores mobiliários e características específicas de cada veículo gerido pela Gestora;
(ii) Relatórios de Risco: Avaliações internas de risco, análises de sensibilidade e projeções relacionadas ao desempenho futuro dos veículos;
(iii) Informações sobre Clientes: Dados pessoais, perfis e dados financeiros dos clientes, bem como histórico de transações e investimentos realizados por eles, mesmo que anonimizados;
(iv) Acordos Contratuais: Termos e condições de contratos, acordos e negociações com parceiros, prestadores de serviços e outras partes envolvidas nas operações;
(v) Relatórios de Auditoria Interna: Resultados de auditorias internas, incluindo recomendações, conclusões e ações corretivas propostas;
(vi) Planejamento Estratégico: Informações sobre estratégias de negócios, metas corporativas, expansão de mercado e desenvolvimento de novos produtos ou serviços;
(vii) Informações Regulatórias Sensíveis: Comunicações com órgãos reguladores, pareceres legais e informações relacionadas a conformidade com as normas do setor; e
(viii) Estrutura Organizacional: Detalhes sobre a estrutura interna da Gestora, incluindo cargos, responsabilidades e informações sobre a equipe de gestão.

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

A divulgação a terceiros não colaboradores ou colaboradores não autorizados da Informação Confidencial é proibida em qualquer circunstância.

A colaboração da Gestora com autoridades fiscalizadoras, a divulgação de Informações Confidenciais a autoridades governamentais por decisões judiciais, arbitrais ou administrativas, requer prévia comunicação ao Diretor de Compliance, Risco e PLD/FTP. Caberá a referido diretor decidir sobre a forma de compartilhamento e sobre a adoção de eventuais medidas administrativas e/ou judiciais relacionadas com a revelação.

Essas diretrizes aplicam-se não apenas durante o relacionamento profissional entre a Gestora e o Colaborador, mas também após seu término. Colaboradores devem manter sigilo sobre Informações Confidenciais, responsabilizando-se por danos em caso de descumprimento, e garantir que os subordinados também o façam e tenham esse mesmo zelo e cuidado com as Informações Confidenciais.

Ao ter acesso a Informações Confidenciais, os Colaboradores devem informar imediatamente o Diretor de Compliance, Risco e PLD/FTP, mencionando a fonte. Isso se aplica mesmo quando a informação é conhecida acidentalmente ou por negligência. Os Colaboradores não devem usar ou divulgar a informação, exceto para o Diretor mencionado.

O uso das Informações Confidenciais para obter vantagem indevida, por negociação de títulos e valores mobiliários, é expressamente proibida, sujeitando o Colaborador a penalidades e possível demissão por justa causa.

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

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.

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

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 o primeiro acesso dos Colaboradores ao ambiente físico da Gestora, será necessário o cadastro prévio no sistema de controle de acesso, com a coleta de dados pessoais e o registro da biometria (impressão digital). Para os acessos subsequentes, será exigida apenas a autenticação biométrica por meio da impressão digital previamente cadastrada.
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, *worms*, *spyware*) nos dispositivos da Gestora. Varreduras constantes identificam e removem qualquer programa que obtenha acesso indevido à rede.

- *Monitoramento e Testes*

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.

  - *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.

  - *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.

  - *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.

- *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.

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

POLÍTICA DE ANTICORRUPÇÃO

A Gestora está comprometida com a conduta ética e transparente em todas as suas atividades. A presente Política de Anticorrupção estabelece os princípios e diretrizes que norteiam a atuação da empresa na prevenção e combate à corrupção, em consonância com a Lei nº 12.846/13 (Lei Anticorrupção) e o Decreto nº 8.420/15.

- *Abrangência*

Esta Política se aplica a todos os Colaboradores da Gestora, incluindo, mas não se limitando a diretores, sócios, Colaboradores, eventuais membros do conselho de administração, acionistas, consultores, prestadores de serviços e demais partes interessadas.

- *Definições*

Para os fins desta Política, considera-se:

(i) Corrupção: qualquer conduta que implique em obtenção de vantagem indevida, direta ou indireta, em razão da função pública exercida pelo agente público;
(ii) Agente Público: qualquer pessoa que exerça cargo, emprego ou função pública, incluindo os membros de qualquer poder;
(iii) Propina: vantagem indevida oferecida ou prometida a agente público, para que ele pratique, omita ou retarde ato de ofício;
(iv) Facilitação de pagamento indevido: vantagem indevida oferecida ou prometida a agente público, para que ele pratique ato de ofício que não seja de seu dever legal;
(v) Peculato: apropriação indébita de dinheiro, valor ou qualquer outro bem público;
(vi) Corrupção Passiva: solicitar ou receber, para si ou para outrem, direta ou indiretamente, vantagem indevida, em razão da função pública exercida;
(vii) Corrupção Ativa: oferecer ou prometer, direta ou indiretamente, vantagem indevida a agente público, para que ele pratique, omita ou retarde ato de ofício.

- *Princípios*

A Política Anticorrupção da Gestora é fundamentada nos seguintes princípios:

(i) Transparência: todas as atividades da Gestora devem ser conduzidas de forma transparente e aberta;
(ii) Integridade: os Colaboradores da Gestora devem agir com honestidade e ética em todas as suas relações;
(iii) Responsabilidade: a Gestora e seus Colaboradores são responsáveis por seus atos e omissões; e
(iv) Zero Tolerância: a Gestora não tolera qualquer tipo de prática corrupta.

- *Código de Conduta*

De forma a buscar sempre as melhores e mais corretas condutas internas pelos Colaboradores da Gestora, é expressamente vedado:

(i) Oferecer, prometer ou dar vantagem indevida a Agente Público;
(ii) Solicitar ou receber vantagem indevida de Agente Público;
(iii) Solicitar ou receber propina;
(iv) Praticar qualquer ato de corrupção, seja ativa ou passiva; e
(v) Participar de qualquer esquema de fraude ou corrupção.

- *Doações a Candidatos e Partidos Políticos*

A Gestora jamais fará doações a candidatos ou partidos políticos, seja diretamente ou por empresas do grupo. As doações individuais dos colaboradores também devem obedecer rigorosamente à legislação em vigor.

- *Relacionamentos com Agentes Públicos*

Em eventuais encontros com Agentes Públicos, tanto internos quanto externos, a Gestora se fará presente por, no mínimo, dois representantes. Estes representantes devem agir com prudência para proteger a Gestora contra condutas ilícitas. Como medida de segurança, os representantes da Gestora devem elaborar relatórios detalhados das interações e apresentá-los ao Diretor de Compliance, Risco e PLD/FTP logo após a sua realização.

- *Canais de Denúncia*

A Gestora disponibiliza canais de denúncia para que seus Colaboradores e demais interessados possam reportar qualquer tipo de prática corrupta. O canal de denúncia interno é compliance@cvpar.com.br.

- *Treinamentos*

A Gestora promove treinamentos periódicos sobre anticorrupção para seus Colaboradores. Os treinamentos abordam temas como:

(i) A Lei Anticorrupção;
(ii) O Código de Conduta da Gestora;
(iii) Os canais de denúncia; e
(iv) As medidas disciplinares cabíveis em caso de violação da Política Anticorrupção.

- *Investigações e Sanções*

Todas as denúncias de práticas corruptas serão apuradas pela Gestora, através de seu Diretor de Compliance, Risco e PLD/FTP. Em caso de confirmação da prática, a Gestora aplicará as

medidas disciplinares cabíveis, que podem incluir:

(i) Advertência verbal;
(ii) Advertência escrita;
(iii) Suspensão;
(iv) Rescisão do contrato de trabalho; ou
(v) Demissão por justa causa.

A Gestora também poderá comunicar o fato às autoridades competentes para a aplicação das sanções legais cabíveis.

- *Revisão e Atualização*

A Política Anticorrupção da Gestora será revisada e atualizada periodicamente para garantir sua adequação às normas legais e às melhores práticas de anticorrupção.

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

POLÍTICAS DE TREINAMENTO

- *Abrangência e Importância*

A Gestora reconhece a importância de manter seus Colaboradores atualizados sobre os princípios éticos, as leis e normas que norteiam suas atividades. Por isso, investe em um programa de treinamento abrangente, que inclui:

(i) Treinamento inicial: obrigatório para todos os Colaboradores, especialmente aqueles com acesso a informações confidenciais ou que participam de decisões de investimento e/ou distribuição de cotas de Fundos geridos pela Gestora; e
(ii) Reciclagem anual: garante que os Colaboradores estejam sempre atualizados sobre as normas, princípios, conceitos e valores da Gestora.

- *Conteúdo Essencial*

O programa de treinamento aborda temas relevantes para o dia a dia da Gestora, como:

(i) Atividades da Gestora: visão geral dos produtos, serviços e processos;
(ii) Princípios éticos e de conduta: código de conduta, valores e responsabilidades dos Colaboradores;
(iii) Normas de compliance: regras e procedimentos para garantir a conformidade com leis e regulamentações;
(iv) Políticas de segregação: medidas para prevenir conflitos de interesse, conforme aplicável;
(v) Confidencialidade, segurança das informações e segurança cibernética: proteção de dados e informações confidenciais da Gestora;
(vi) Código de Ética e Política de Investimentos Pessoais: diretrizes para o comportamento dos Colaboradores;
(vii) Penalidades por descumprimento das regras: medidas disciplinares cabíveis; e
(viii) Leis e normas aplicáveis: legislação relevante para as atividades da Gestora.

- *Responsabilidades e Implementação*

O Diretor de Compliance, Risco e PLD/FTP é responsável por:

(i) Implementar o programa de treinamento: definir datas, horários, conteúdo e materiais;
(ii) Garantir a participação dos Colaboradores: monitorar a assiduidade e o engajamento; e
(iii) Contratar profissionais especializados: quando necessário, para ministrar treinamentos específicos.

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

O sucesso do programa depende do comprometimento de todos os Colaboradores com:

(i) Participação ativa nos treinamentos: dedicar tempo e atenção ao conteúdo apresentado;
(ii) Aplicação dos conhecimentos no dia a dia: agir de acordo com as normas e princípios da empresa; e
(iii) Comportamento ético e profissional: manter conduta exemplar em todas as atividades.

Ao investir na capacitação de seus Colaboradores, a Gestora constrói um ambiente de trabalho ético, profissional e comprometido com o sucesso.

Data da Atualização	Responsável	Versão
Março de 2026	Diretor de Compliance, Risco e PLD/FTP	1ª

POLÍTICA DE CERTIFICAÇÃO

- *Visão Geral*

A Gestora, como administradora de recursos de terceiros e distribuidora dos fundos que gere, segue o Código de AGRT, que descontinuou o Código ANBIMA de Certificação. Nesse sentido, todos os colaboradores que possuem o poder de tomada de decisão de investimentos e desinvestimentos nos veículos geridos pela Gestora necessariamente precisam ter as certificações ANBIMA CGA e/ou CGE.

Adicionalmente, tendo em vista a atuação da Gestora como distribuidora dos fundos sob sua gestão, esta identificou, segundo o Código de Certificação, que a certificação profissional ANBIMA série 20 ("CPA-20"), qual fora substituída pelo Certificado Profissional ANBIMA de Relacionamento ("C-PRO R"), é a certificação pertinente para os Colaboradores que realizam a distribuição dos fundos diretamente junto a investidores. Inobstante, a Gestora assegura que todos os seus Colaboradores que possuem a certificação CPA-20 farão o curso de transição de certificação da ANBIMA, de maneira tempestiva, para possuírem o C-PRO R de maneira regular.

- *Identificação de Profissionais Certificados*

(i) Antes da contratação, o cargo e as funções do potencial colaborador serão avaliados pela Área de Compliance para determinar a necessidade de certificação; e
(ii) O Diretor de Compliance, Risco e PLD/FTP verificará a certificação ou isenção do potencial colaborador antes de sua admissão.

- *Rotinas de Verificação*

(i) **Anualmente**, o Diretor de Compliance, Risco e PLD/FTP verificará a validade das certificações dos Colaboradores;
(ii) O Diretor de Compliance, Risco e PLD/FTP verificará anualmente se há alterações nas funções dos colaboradores e se há necessidade de atualização dos sistemas aplicáveis;
(iii) O Colaborador será notificado para renovar a certificação antes do vencimento pela Área de Compliance da Gestora;
(iv) Colaboradores sem CGA/CGE **não** podem atuar com poder de tomada de decisão de investimentos e desinvestimentos nos veículos geridos pela Gestora;
(v) Colaboradores sem CPA-20 e/ou C-PRO R, conforme aplicável, **não** podem atuar na distribuição dos fundos de investimento diretamente junto a investidores; e
(vi) Irregularidades na certificação podem levar ao afastamento do Colaborador e apuração de responsabilidades.

- *Treinamento e Afastamento*

(i) Assuntos de certificação serão abordados no treinamento anual de compliance. Adicionalmente, no ingresso de cada Colaborador, este terá a oportunidade de sanar todas as suas dúvidas com a Área de Compliance a respeito dos temas referentes as certificações;

(ii) Profissionais não certificados ou em processo de certificação serão afastados das atividades elegíveis; e

(iii) Profissionais que deixam a empresa devem assinar um termo de afastamento, conforme modelo constante no Anexo IV.

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 HIERON 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 HIERON 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 HIERON INVESTIMENTOS LTDA

Testemunhas:

1._____ 2._____

Nome: Nome:
CPF: CPF:

ANEXO III
TERMO DE PROPRIEDADE INTELECTUAL

Pelo presente instrumento, Eu, [Nome Completo do Colaborador], CPF [Número do CPF do Colaborador], RG [Número do RG do Colaborador], colaborador da **CVPAR HIERON INVESTIMENTOS LTDA.** ("Gestora"), declaro que:

(i) A entrega dos documentos à Gestora, em pen drive da marca [•] e número de série [•] ("Documentos"), não viola nenhum contrato, acordo de confidencialidade ou direito de propriedade intelectual de terceiros;
(ii) Concorda que qualquer modificação nos Documentos será de propriedade exclusiva da Gestora; e
(iii) Não poderá usar os Documentos modificados após o desligamento da Gestora, salvo com autorização expressa.

Os pen-drives e a lista de arquivos constantes neles integram este termo para todos os fins de direito. Para maiores informações, consultar o apêndice abaixo.

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

Assinatura: _____ (Nome do Colaborad

ANEXO VI
TERMO DE AFASTAMENTO

Pelo presente instrumento, Eu, [Nome Completo do Colaborador], CPF [Número do CPF do Colaborador], RG [Número do RG do Colaborador], colaborador da **CVPAR HIERON INVESTIMENTOS LTDA.** ("Gestora"), declaro que, a partir desta data, estou afastado das atividades de gestão e/ou de distribuição de fundos próprios da Gestora por prazo indeterminado:

(i) até que obtenha a Certificação ANBIMA [CGA/CGE];

(ii) até que obtenha a Certificação ANBIMA [C-PRO R];

(iii) considerando que não faço mais parte da composição funcional da Gestora.

Local e Data: [Local e Data de Assinatura do Termo]

Assinatura: _____ (Nome do Colaborador)