HORIZONTES ASSET LTDA.

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão	Data-base	Aprovação	Próxima revisão
1.1	Maio/2026	Diretoria Executiva	Anual (maio/2027)

1. Objeto e escopo

A presente Política de Segurança Cibernética (“Política”) tem por objeto estabelecer os princípios, as diretrizes, os controles e as responsabilidades aplicáveis à proteção dos ativos de informação da HORIZONTES ASSET LTDA. (“Horizontes” ou “Gestora”), inscrita no CNPJ sob o nº 58.805.121/0001-90, contra ameaças cibernéticas, falhas técnicas, uso indevido e violações à confidencialidade, integridade e disponibilidade da informação.

Esta Política é emitida em atendimento (i) ao art. 16 da Resolução CVM nº 21/2021; (ii) à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais “LGPD”); (iii) às Diretrizes ANBIMA aplicáveis a controles internos e segurança da informação; e (iv) às melhores práticas internacionais de gestão de segurança da informação, em especial os princípios consagrados na ISO/IEC 27001.

O escopo desta Política abrange todos os ativos de informação utilizados pela Gestora, em qualquer formato (digital, físico, impresso ou verbal), incluindo: (i) sistemas, dispositivos, redes e serviços em nuvem; (ii) bases de dados de investidores, contrapartes e fundos sob gestão; (iii) informação confidencial sobre estratégias de investimento; (iv) credenciais de acesso e ativos criptográficos; e (v) qualquer dado pessoal tratado no curso da atividade. Aplica-se a todos os sócios, diretores, empregados, estagiários, prestadores de serviços e demais terceiros com acesso aos ativos da Gestora.

2. Princípios gerais e classificação da informação

2.1. Princípios

A gestão da segurança cibernética na Horizontes observa os seguintes princípios fundamentais:

- Confidencialidade: a informação é acessível apenas a quem dela legitimamente necessite no exercício de sua função;
- Integridade: a informação é preservada em sua exatidão e completude, sem alteração não autorizada;
- Disponibilidade: a informação está disponível aos usuários autorizados sempre que necessário ao desempenho de suas atribuições;
- Rastreabilidade: todas as ações relevantes sobre ativos de informação são registradas e auditáveis;
- Menor privilégio: cada usuário possui apenas os acessos estritamente necessários ao desempenho de suas funções;
- Defesa em profundidade: múltiplas camadas de controle protegem cada ativo crítico, evitando ponto único de falha.

2.2. Classificação da informação

Os ativos de informação são classificados em quatro níveis, observada a sensibilidade do conteúdo:

Classificação	Descrição	Exemplos
Pública	Informação destinada à divulgação ampla, sem restrição.	Política publicada no site, conteúdo institucional, formulário de referência.
Interna	Informação de uso restrito ao corpo funcional da Gestora.	Procedimentos internos, comunicados corporativos, agenda de eventos.
Confidencial	Informação cuja divulgação não autorizada produz dano relevante à Gestora, a investidores ou a contrapartes.	Estratégias de investimento, posições dos fundos, dados de investidores, modelos quantitativos.
Restrita	Informação cujo vazamento gera impacto material, regulatório ou reputacional severo.	Credenciais, chaves criptográficas, dados pessoais sensíveis, segredos de negócio.

3. Controles técnicos

A Gestora adota o seguinte conjunto mínimo de controles técnicos, aplicáveis à proteção dos ativos de informação:

3.1. Controle de acesso e gestão de identidade

A Gestora adota Active Directory corporativo como mecanismo central de gestão de identidade, com dois controladores de domínio redundantes hospedados em zonas de disponibilidade distintas no provedor de nuvem contratado, garantindo continuidade da autenticação corporativa. O acesso remoto à infraestrutura é realizado exclusivamente por VPN site-to-client com autenticação multifator (MFA) baseada em TOTP (Time-based One-Time Password), integrada ao Active Directory. Em complemento:

- Autenticação individualizada para todo usuário com acesso aos sistemas da Gestora, vedado o uso de credenciais compartilhadas;
- Política de senhas fortes, com complexidade mínima, rotação periódica e bloqueio após tentativas de acesso malsucedidas;
- Revisão semestral da lista de usuários ativos e seus respectivos privilégios, conduzida pelo Diretor de Compliance, Risco e PLD em conjunto com o prestador de TI, com revogação imediata de acessos de pessoas desligadas;
- Princípio do menor privilégio aplicado a todos os perfis de acesso, com permissões NTFS baseadas em grupos do Active Directory e Group Policies (GPOs) corporativas.

3.2. Criptografia

- Criptografia em trânsito (TLS atualizado) para todas as comunicações sensíveis, incluindo o canal VPN com MFA;
- Criptografia em repouso para informação classificada como confidencial ou restrita armazenada nos volumes do provedor de nuvem corporativo;
- Custódia segura de chaves criptográficas, vedada sua disponibilização em texto aberto ou em ambiente não controlado.

3.3. Infraestrutura de rede e proteção de perímetro

A infraestrutura corporativa da Gestora é hospedada em provedor de nuvem (Amazon Web Services - AWS), em arquitetura Virtual Private Cloud (VPC) dedicada com segmentação por subnets públicas e privadas, distribuída em múltiplas zonas de disponibilidade (Multi-AZ) para fins de redundância. O perímetro de rede é protegido por firewall dedicado (OPNsense), com regras de entrada e saída segmentadas por camada

funcional (aplicação, identidade, perímetro) e Security Groups específicos por componente. Aplicam-se ainda:

- Solução de antivírus e antimalware ativa, atualizada e monitorada em todos os dispositivos corporativos;
- Sistema operacional e aplicativos sempre atualizados, com aplicação tempestiva de correções de segurança (patches), inclusive nas instâncias de servidor hospedadas em nuvem;
- Vedação ao uso de redes Wi-Fi públicas para acesso a sistemas que tratem informação confidencial ou restrita, salvo mediante uso de VPN corporativa;
- Bloqueio automático de tela em dispositivos corporativos após período de inatividade.

3.4. Backup e recuperação

Os backups dos sistemas críticos da Gestora são executados de forma automatizada por meio de serviço de backup gerenciado do provedor de nuvem (AWS Backup), com política configurada para os volumes e recursos críticos, incluindo controladores de domínio, file server e instâncias de aplicação. Aplicam-se ainda:

- Frequência, retenção e janela de backup definidas conforme criticidade dos sistemas e exigências regulatórias e contratuais;
- Armazenamento dos backups em ambiente segregado, com redundância intra-região;
- Teste de restauração realizado, no mínimo, semestralmente, para garantir efetividade dos backups.

3.5. Monitoramento e registros

O monitoramento contínuo da infraestrutura é realizado por meio de serviço de observabilidade do provedor de nuvem (Amazon CloudWatch), com dashboards configurados para acompanhamento de métricas de CPU, memória, disco e rede, e alarmes que disparam notificações automáticas por e-mail diante de eventos críticos. Em complemento:

- Registros (logs) de acesso e de eventos relevantes mantidos por prazo compatível com a finalidade de auditoria e investigação de incidentes;
- Monitoramento de tentativas anômalas de acesso e de uso indevido dos sistemas;
- Tratamento dos registros como informação confidencial, com acesso restrito ao Diretor de Compliance, Risco e PLD e ao prestador de TI.

4. Controles organizacionais

4.1. Treinamento e conscientização

Todos os sócios, diretores, empregados, estagiários e prestadores com acesso a ativos de informação da Gestora participam de programa de conscientização em segurança cibernética, com periodicidade mínima anual, abordando, entre outros temas: engenharia social, phishing, gestão de senhas, classificação da informação, uso de dispositivos pessoais (BYOD), tratamento de dados pessoais (LGPD) e procedimento para reporte de incidentes.

4.2. Termo de responsabilidade

Todo profissional com acesso a ativos de informação assina termo de responsabilidade e confidencialidade, no qual reconhece esta Política, o Código de Ética e Conduta e as demais normas internas aplicáveis, assumindo o compromisso de zelar pela segurança da informação.

4.3. Uso de dispositivos pessoais

O uso de dispositivos pessoais (BYOD - bring your own device) para acesso a sistemas da Gestora é permitido apenas mediante: (i) prévia autorização do responsável por TI; (ii) implementação dos controles mínimos previstos no item 3 desta Política; e (iii) reconhecimento expresso, pelo usuário, da possibilidade de remoção remota de dados corporativos do dispositivo em caso de perda, roubo ou desligamento.

5. Gestão de fornecedores de TI e serviços em nuvem

5.1. Princípios gerais

A contratação de fornecedores que prestem serviços de tecnologia da informação à Gestora, ou que tratem ativos de informação por conta dela, observa os seguintes critérios mínimos:

- Avaliação prévia da reputação, da idoneidade e da capacidade técnica do fornecedor;
- Verificação da existência de políticas próprias de segurança da informação compatíveis com as exigências desta Política;
- Existência, sempre que aplicável, de certificações reconhecidas (ISO/IEC 27001, SOC 2 ou equivalentes);
- Inclusão, no contrato firmado com o fornecedor, de cláusulas sobre confidencialidade, tratamento de dados pessoais (operador, na forma da LGPD),

prazo e forma de notificação de incidentes, direito de auditoria e procedimento para devolução ou destruição de informações ao final do contrato;

- Reavaliação periódica do fornecedor, no mínimo anual, ou sempre que ocorrer alteração relevante no escopo dos serviços contratados.

5.2. Prestadores críticos de tecnologia da informação

Na data-base desta Política, a Gestora mantém os seguintes prestadores críticos formalmente contratados para suporte à sua infraestrutura e operação de tecnologia da informação:

Prestador	Objeto contratado	Vínculo contratual
BAlves Gestão em Tecnologia da Informação	Implantação e arquitetura da infraestrutura cloud corporativa em AWS, contemplando VPC Multi-AZ, Active Directory redundante, file server, firewall OPNsense, VPN com MFA, AWS Backup automatizado e monitoramento via CloudWatch.	Proposta Comercial PROP-2026-001, aceite formal pela Diretoria Executiva da Gestora em 24/04/2026.
Manucom Tecnologia Ltda.	Suporte técnico em tecnologia da informação, incluindo manutenção preventiva e corretiva dos equipamentos da Gestora, com atendimento remoto e presencial, em horário 5x8 (segunda a sexta, 9h às 18h) e SLAs por gravidade do incidente.	Contrato de Suporte Técnico nº 357-2026, assinado eletronicamente em 30/04/2026 (D4Sign / ICP-Brasil), vigência iniciada em 01/03/2026, prazo indeterminado. Contrato originalmente firmado em nome de ENGE ASSET LTDA. (atual HORIZONTES ASSET LTDA., mesmo CNPJ).
Nullpointer	Fornecimento da plataforma operacional especializada NPFlow (orquestração de fluxos sobre engine BPMN) + Sentinela (camada cognitiva de vigilância sobre corpus regulatório do segmento) + Gestora App (tela única operacional), voltada à execução, controle e monitoramento das atividades de gestão de FIDC.	Contratação em fase de formalização contratual e implantação técnica, observado o escopo previsto no material técnico de diligência da fornecedora.

Os instrumentos contratuais firmados com os prestadores acima preveem, conforme aplicável: (i) níveis de serviço (SLAs) definidos por gravidade do incidente, sendo de até 4 (quatro) horas para incidentes graves no caso do suporte técnico; (ii) procedimentos formais para abertura, registro e baixa de chamados técnicos; (iii) atribuição clara de

responsabilidades; (iv) cláusulas de confidencialidade; e (v) regime de reavaliação periódica pela Diretoria de Compliance, Risco e PLD.

6. Resposta a incidentes de segurança

Esta Política é complementada pelo Plano de Continuidade de Negócios (BCP) da Gestora, em especial quanto aos cenários C1 (Falha de TI) e C5 (Incidente cibernético) e respectivos procedimentos de resposta.

Sem prejuízo do disposto no BCP, observa-se o seguinte fluxo geral diante de incidente cibernético:

Fase	Procedimento
1. Detecção	Identificação do incidente por monitoramento (CloudWatch ou outro), alerta automatizado ou reporte de usuário. Comunicação imediata ao prestador de TI e ao Diretor de Compliance, Risco e PLD.
2. Contenção	Isolamento dos sistemas afetados, troca imediata de credenciais comprometidas, preservação de evidências para análise técnica e eventual investigação.
3. Erradicação	Identificação e remoção da causa-raiz do incidente, com apoio do prestador de TI e, quando necessário, de prestador especializado em resposta a incidentes.
4. Recuperação	Restauração dos sistemas a partir de backups íntegros (AWS Backup), teste de funcionalidade e retorno controlado à operação normal.
5. Comunicação	Comunicação a stakeholders, observado o Plano de Comunicação previsto no BCP, com avaliação específica sobre obrigação de comunicação à ANPD (em caso de incidente com dados pessoais), à CVM, à ANBIMA e aos titulares afetados.
6. Lições aprendidas	Registro do incidente em base interna, análise crítica, identificação de oportunidades de melhoria e atualização desta Política e do BCP, se aplicável.

7. Tratamento de dados pessoais e LGPD

A Gestora reconhece a Lei nº 13.709/2018 (LGPD) como aplicável às suas atividades, na qualidade de controladora ou de operadora de dados pessoais, conforme o caso, e adota os seguintes compromissos:

- Tratamento de dados pessoais somente para finalidades legítimas, específicas e informadas ao titular;

- Adoção dos princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas;
- Adoção de medidas técnicas e administrativas adequadas para proteção dos dados pessoais contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Manutenção de registro das operações de tratamento de dados pessoais (RTOTDP), observado o disposto no art. 37 da LGPD;
- Comunicação à ANPD e ao titular sobre incidentes que possam acarretar risco ou dano relevante, em prazo razoável, conforme orientação da ANPD.

7.1. Encarregada pelo Tratamento de Dados Pessoais (DPO)

A Encarregada pelo Tratamento de Dados Pessoais (DPO) da Gestora, designada nos termos do art. 41 da Lei nº 13.709/2018, é Natália Uchôa Brandão, Diretora de Compliance, Risco e PLD. As informações de contato da Encarregada, para fins de exercício de direitos pelos titulares de dados, são divulgadas em local de acesso público e gratuito na página eletrônica da Gestora (horizontesasset.com).

8. Vedações e responsabilidades dos usuários

É vedado a todos os usuários, sem exceção:

- Compartilhar credenciais de acesso pessoais com terceiros, ainda que internos à Gestora;
- Acessar, copiar ou divulgar informação confidencial ou restrita fora do exercício regular de suas funções;
- Instalar softwares ou aplicações não autorizadas em dispositivos corporativos;
- Desativar, contornar ou tentar burlar controles de segurança implementados pela Gestora;
- Utilizar recursos da Gestora para fins ilícitos, antiéticos ou contrários ao Código de Ética e Conduta;
- Tratar dados pessoais para finalidade diversa daquela autorizada pelo titular ou pela legislação aplicável.

O descumprimento desta Política sujeita o infrator às medidas disciplinares previstas no Código de Ética e Conduta e no Manual de Compliance da Gestora, sem prejuízo das responsabilidades civil, administrativa e penal aplicáveis.

9. Testes, atualização e divulgação

Esta Política é submetida aos seguintes ciclos de manutenção:

- Revisão ordinária anual, conduzida pela Diretora de Compliance, Risco e PLD em conjunto com os prestadores de TI;
- Revisão extraordinária sempre que houver: (i) incidente cibernético relevante, (ii) alteração regulatória relevante (CVM, ANBIMA, ANPD), (iii) mudança material na infraestrutura de TI ou no porte da Gestora, (iv) substituição ou inclusão de prestador crítico, ou (v) determinação de regulador ou autorregulador;
- Teste anual obrigatório de pelo menos um controle técnico crítico (por exemplo: restauração de backup via AWS Backup, simulação de phishing, teste de invasão controlado), com registro do resultado em relatório interno.

Após cada revisão, esta Política será disponibilizada em sua versão atualizada na página eletrônica da Gestora (horizontesasset.com), em local de acesso público e gratuito.

10. Aprovação, vigência e publicação

A presente Política de Segurança Cibernética foi aprovada pela Diretoria Executiva da Horizontes Asset Ltda. e entra em vigor na data de sua publicação, permanecendo válida até a sua próxima revisão ordinária ou extraordinária, observado o disposto no item 9 acima.

11. Assinaturas

São Paulo, 19 de maio de 2026.

IRAPUA DE CARVALHO DANTAS:00800251458

Assinado de forma digital por IRAPUA DE CARVALHO DANTAS:00800251458

Irapuã de Carvalho Dantas
Diretor Executivo
Horizontes Asset Ltda.

Natália Uchôa Brandão
Diretora de Compliance, Risco e PLD
Encarregada pelo Tratamento de Dados Pessoais (DPO) - Horizontes Asset Ltda.