



CARTOR CAPITAL
GESTÃO DE RECURSOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS

CARTOR CAPITAL GESTÃO DE RECURSOS LTDA.
(“Sociedade”)

Vigência e última revisão: **Agosto/2026**

CAPÍTULO I

Objetivo e Base Normativa

1.1. Esta Política define as regras e os princípios norteadores das condutas dos colaboradores da Sociedade em matéria de segurança da informação, segurança cibernética e proteção de dados pessoais.

1.2. Esta Política observa a Lei nº 13.709/18, a regulamentação editada pela Autoridade Nacional de Proteção de Dados, a Resolução CVM nº 21, as Regras e Procedimentos de Deveres Básicos da ANBIMA, em especial os seus artigos 9º, 11, 13, 14, 15, 16 e 17, e as diretrizes do Guia ANBIMA de Segurança Cibernética.

1.3. Os colaboradores formalizam ciência do inteiro teor desta Política mediante assinatura do Termo de Adesão e Confidencialidade constante do Código de Ética e Conduta, sendo submetidos anualmente ao Programa de Treinamento adotado pela Sociedade.

1.4. A Sociedade coletará Termo de Confidencialidade de quaisquer terceiros contratados que tiverem acesso a informações confidenciais, salvo se o compromisso já constar do respectivo contrato de prestação de serviços.

1.5. Em caso de dúvida, o colaborador deve buscar auxílio junto ao Diretor de Risco, Compliance e PLD, devendo as questões de infraestrutura tecnológica ser tratadas com o responsável pela Tecnologia da Informação.

CAPÍTULO II

Segurança da Informação

2.1. Informações confidenciais e privilegiadas. Consideram-se confidenciais todas as informações relativas à Sociedade, aos veículos sob gestão, aos investidores, aos colaboradores e às contrapartes que não sejam de domínio público, incluindo: composição e movimentação das carteiras; teses, análises e estudos de investimento; ordens emitidas e a emitir; dados cadastrais e financeiros de investidores; informações societárias e financeiras da Sociedade; e dados pessoais de qualquer natureza. Consideram-se privilegiadas as informações relevantes ainda não divulgadas ao mercado, cuja utilização é vedada nos termos do Código de Ética e Conduta.

2.2. Processo de preservação e acesso. O acesso às informações confidenciais e privilegiadas é concedido conforme o princípio da necessidade de conhecer, restrito às áreas e aos profissionais cujas atribuições o justifiquem, incluídos os terceiros contratados que a elas devam ter acesso. A concessão, a alteração e a revogação de acessos são formalizadas e registradas, competindo ao responsável pela Tecnologia da Informação sua execução e ao Compliance sua revisão.

2.3. O gerenciamento de identidade e acesso observa o ciclo completo do relacionamento do profissional com a Sociedade, do início ao término, inclusive nos casos de mudança de atividade, com revisão imediata dos acessos no desligamento e no gozo de férias.

2.4. Ações de proteção, prevenção e controle. Para mitigar o risco de vazamento de informações confidenciais e privilegiadas, a Sociedade adota: controles de acesso físico e lógico; segregação física e lógica dos ambientes; autenticação multifator, sempre que tecnicamente disponível, no acesso ao correio eletrônico corporativo, no acesso remoto à

rede e nos sistemas que contenham informações confidenciais, dados pessoais ou dados das carteiras; política de senhas com troca periódica; bloqueio automático de tela por inatividade; vedação ao uso de aplicações não autorizadas; e monitoramento das ferramentas de comunicação utilizadas para contato com agentes externos.

2.5. Mecanismos de controle e monitoramento. Os eventos de acesso, autenticação e alteração de senhas são rastreáveis e auditáveis, com trilha de auditoria habilitada e análise diária de registros. Qualquer inconsistência é reportada imediatamente ao Diretor de Risco, Compliance e PLD.

2.6. Testes. A Sociedade realiza testes do programa de segurança da informação com periodicidade semestral, abrangendo a verificação dos controles de acesso, a restauração de dados a partir do backup e a simulação de resposta a incidentes.

2.7. Plano de resposta a incidentes de segurança da informação. Identificado incidente, o Diretor de Risco, Compliance e PLD coordena a apuração dos fatos, determina o isolamento dos ativos afetados, aciona a restauração a partir do backup, avalia a extensão do dano e implementa os procedimentos corretivos e de responsabilização. Sem prejuízo do disposto no Plano de Continuidade de Negócios, o plano de resposta visa assegurar a continuidade das atividades ou a recuperação adequada nos casos mais graves.

2.8. Utilização de bens e equipamentos. Os equipamentos, sistemas, correio eletrônico e demais recursos tecnológicos disponibilizados pela Sociedade destinam-se ao exercício das atividades profissionais, sujeitando-se a revisão e monitoramento a qualquer tempo, sem aviso prévio, de forma a detectar irregularidade na transferência de informações.

2.9. Documentos físicos. Os colaboradores devem evitar o esquecimento de documentos em mesas, bancadas e impressoras, e proceder ao descarte seguro de documentos que contenham informações confidenciais.

CAPÍTULO III

Proteção de Dados Pessoais

3.1. Este Capítulo regula o tratamento de dados pessoais e de dados pessoais sensíveis pela Sociedade, assim considerada toda operação realizada com tais dados, tais como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

3.2. Consideram-se dados pessoais quaisquer informações relacionadas a pessoa natural identificada ou identificável, inclusive as utilizadas para a formação de perfil comportamental. Consideram-se dados pessoais sensíveis os que versem sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual e dado genético ou biométrico, quando vinculados a uma pessoa natural.

3.3. Todos os dados pessoais são informações confidenciais e recebem o tratamento previsto no Capítulo II.

3.4. O tratamento observa a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

3.5. O tratamento somente será realizado nas seguintes hipóteses: (i) cumprimento de obrigação legal ou regulatória; (ii) execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido deste; (iii) atendimento a interesses legítimos da Sociedade ou de terceiros, exceto quando prevalecerem direitos e liberdades fundamentais do titular; (iv) fornecimento de consentimento pelo titular; ou (v) exercício regular de direitos em processo judicial, administrativo ou arbitral.

3.6. Ciclo de vida do dado. A Sociedade assegura a integridade, a confidencialidade e a disponibilidade dos ativos de informação e dos dados pessoais durante todo o seu ciclo de vida, da geração ao descarte, incluindo o armazenamento, o acesso, o tratamento, a transmissão e o transporte, adotando, em cada etapa, controles proporcionais à classificação da informação.

3.7. O consentimento, quando aplicável, deve constar de cláusula destacada, referir-se a finalidades determinadas, ser revogável a qualquer tempo por procedimento gratuito e facilitado, e o dado obtido mediante consentimento somente poderá ser compartilhado com terceiros mediante autorização expressa do titular.

3.8. O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, disponibilizadas de forma clara, adequada e ostensiva, incluindo a finalidade específica, a forma e a duração do tratamento, a identificação e o contato do controlador, as informações sobre eventual compartilhamento, as responsabilidades dos agentes de tratamento e os direitos previstos no artigo 18 da Lei Geral de Proteção de Dados.

3.9. O término do tratamento ocorre quando verificado que a finalidade foi alcançada ou que os dados deixaram de ser necessários; ao fim do período de tratamento, correspondente a 5 (cinco) anos após a cessação da prestação de serviço ao titular; por comunicação do titular, inclusive no exercício do direito de revogação do consentimento, resguardado o interesse público; ou por determinação da autoridade nacional.

3.10. Os dados são eliminados após o término do tratamento, autorizada a conservação para cumprimento de obrigação legal ou regulatória, para transferência a terceiro observados os requisitos aplicáveis, ou para uso exclusivo da Sociedade, vedado o acesso por terceiro e desde que anonimizados.

3.11. A Sociedade mantém registro das operações de tratamento que realizar, especialmente quando fundadas em legítimo interesse, e detalha, em documento próprio, o controlador, o operador, as bases legais, a finalidade, a duração do tratamento, o compartilhamento e as responsabilidades.

3.12. O encarregado pelo tratamento de dados pessoais é o Diretor de Risco, Compliance e PLD, cujas informações de contato estão disponíveis no sítio eletrônico da Sociedade. A Política de Privacidade da Sociedade está permanentemente disponível para consulta pública no mesmo sítio eletrônico, em local de destaque e de fácil acesso.

3.13. Incidentes envolvendo dados pessoais. Ocorrido incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o Diretor de Risco, Compliance e PLD comunicará a Autoridade Nacional de Proteção de Dados e os titulares afetados no prazo de 3 (três) dias úteis contados do conhecimento de que o incidente afetou dados pessoais, por meio do formulário eletrônico disponibilizado pela autoridade. Não dispondo de informações completas no prazo, a comunicação poderá ser realizada de

forma preliminar, com justificativa, complementando-se as informações em até 20 (vinte) dias úteis.

3.14. A Sociedade mantém registro de todos os incidentes de segurança envolvendo dados pessoais, inclusive dos não comunicados, pelo prazo mínimo de 5 (cinco) anos, com indicação da data do conhecimento, da descrição e da causa do incidente, dos dados e titulares afetados, das medidas adotadas e, quando for o caso, dos motivos da ausência de comunicação.

CAPÍTULO IV

Identificação e Avaliação de Riscos Cibernéticos

4.1. A identificação e a avaliação de riscos cibernéticos visam evitar incidentes relevantes que afetem os processos críticos do negócio, os dados e as informações sensíveis, ou que tenham impacto significativo sobre as atividades da Sociedade.

4.2. Ativos relevantes. São considerados ativos relevantes: as estações de trabalho e equipamentos portáteis; os servidores e o ambiente de nuvem corporativa; a rede e os equipamentos de borda; o correio eletrônico corporativo; os sistemas proprietários de gestão, risco e enquadramento; os sistemas de terceiros utilizados na atividade; as bases de dados de carteiras, investidores e colaboradores; e os processos de emissão e registro de ordens.

4.3. Vulnerabilidades e ameaças. São consideradas ameaças, entre outras: código malicioso; engenharia social; pharming; phishing; vishing; smishing; acesso físico não autorizado; ataques de negação de serviço; e invasões persistentes. As vulnerabilidades internas e externas associadas a cada ativo são identificadas, avaliadas quanto à probabilidade de ocorrência e à magnitude do impacto, e revisadas sempre que houver alteração relevante na estrutura tecnológica.

4.4. A Sociedade mantém inventário atualizado de hardware e software e realiza verificações semestrais para identificar elementos estranhos, tais como equipamentos não autorizados ou softwares não licenciados. Sempre que houver alteração relevante na estrutura tecnológica, são realizadas análises de vulnerabilidade.

CAPÍTULO V

Ações de Proteção e Prevenção e Mecanismos de Supervisão

5.1. São adotadas as seguintes medidas preventivas por risco identificado:

- (i) Indisponibilidade dos arquivos na rede — redundância para assegurar a disponibilidade dos sistemas;
- (ii) Perda de arquivos de usuários — backup diário em nuvem de todos os dados armazenados no servidor;
- (iii) Acesso indevido a aplicações restritas — troca trimestral das senhas de alta criticidade, trilha de auditoria habilitada e disponibilização desta Política aos usuários;
- (iv) Tentativa de invasão da rede interna — análise de todo o tráfego de entrada pelo firewall, com bloqueio proativo de acessos suspeitos e alerta ao responsável pela Tecnologia da Informação;

(v) Phishing e engenharia social — varredura de antivírus, filtro de conteúdo, treinamento periódico e simulações;

(vi) Colaboradores desligados com credenciais ativas — revisão imediata dos acessos e manutenção do registro.

5.2. Todos os novos equipamentos e sistemas instalados devem contar com as configurações de proteção descritas nesta Política, sendo realizado teste em ambiente de homologação antes do início de sua utilização. Semestralmente são realizadas inspeções para verificação da atualização dos sistemas operacionais e dos softwares instalados.

5.3. Todos os programas de computador utilizados pelos colaboradores devem ser previamente autorizados pelo responsável pela Tecnologia da Informação, sendo vedadas aplicações não autorizadas.

5.4. São realizados os seguintes testes de verificação, para identificação de anomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados: backup diário; teste de restauração de dados semanal; teste de invasão externa e phishing semestral; simulação de resposta a incidentes com cenários semestral; e análise de registros e trilhas de auditoria diária.

5.5. Mecanismos de acompanhamento e validação. A Sociedade mantém mecanismos de acompanhamento destinados a assegurar a implementação e a efetividade das regras, procedimentos e controles previstos nos Capítulos II, III e IV, contemplando: os processos e controles adotados no acompanhamento; a definição de metodologias, métricas, critérios e indicadores; e a identificação e a correção de eventuais deficiências.

5.6. Os mecanismos de que trata o item anterior incluem validação e testes com periodicidade mínima anual, destinados a avaliar se as medidas de sigilo, proteção de dados e segurança cibernética são capazes de suportar de modo satisfatório os processos operacionais, sistemas e bancos de dados críticos, manter sua integridade, segurança e consistência, e verificar se os planos podem ser ativados tempestivamente.

5.7. Independência da validação. Os resultados da validação anual de que trata o item 5.6, bem como os resultados dos testes previstos no item 5.4, são reportados ao Comitê de Risco e Compliance, e não exclusivamente à área responsável por sua execução, de modo a assegurar a segregação entre a execução dos controles e a sua supervisão.

CAPÍTULO VI

Contratação de Processamento e Armazenamento de Dados e Computação em Nuvem

6.1. A contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, observa o disposto neste Capítulo, sem prejuízo das regras da Política de Seleção, Contratação e Monitoramento de Prestadores de Serviços.

6.2. Previamente à contratação, a Sociedade classifica o serviço quanto à criticidade, considerando a natureza dos dados envolvidos, a relevância do serviço para as atividades essenciais e o impacto de sua indisponibilidade. Serviços classificados como críticos ou de maior risco submetem-se integralmente à verificação prevista no item 6.3.

6.3. A contratação assegura a verificação da capacidade do potencial prestador, incluindo, no mínimo:

- (i) o acesso da Sociedade aos dados e às informações a serem processados ou armazenados pelo prestador;
- (ii) a confidencialidade, a integridade, a disponibilidade e a recuperação das informações e dados processados ou armazenados;
- (iii) a aderência do prestador às certificações exigidas pela Sociedade ou pelos reguladores para a prestação do serviço, quando aplicável;
- (iv) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços prestados;
- (v) a identificação e a segregação dos dados de clientes, colaboradores e terceiros relevantes por meio de controles físicos ou lógicos; e
- (vi) a qualidade dos controles de acesso voltados à proteção dos dados e das informações de clientes, colaboradores e terceiros relevantes.

6.4. A Sociedade utiliza, para a verificação de que trata o item anterior, questionário de diligência específico, admitido o modelo disponibilizado pela ANBIMA, cujo resultado é arquivado com a documentação da contratação.

6.5. A localização geográfica dos dados, as condições de portabilidade e de devolução em caso de encerramento do contrato e os procedimentos aplicáveis em caso de incidente no prestador são verificados previamente e registrados.

6.6. Os prestadores contratados nos termos deste Capítulo integram a base de prestadores submetida à supervisão baseada em risco prevista na Política de Seleção, Contratação e Monitoramento de Prestadores de Serviços.

CAPÍTULO VII

Resposta a Incidentes Cibernéticos

7.1. A Sociedade adota os seguintes planos de ação de resposta, em função das ameaças identificadas: perda ou corrupção de arquivo na rede, de severidade alta, com restauração a partir do backup; falha de backup, de severidade alta, com tratativa da falha e novo agendamento; compartilhamento de senhas, de severidade alta, com treinamento e revisão de credenciais; tentativa de invasão, de severidade alta, com análise dos registros do firewall e mitigação; phishing, de severidade alta, com varredura de antivírus, troca de senha e verificação da integridade do equipamento; e credenciais ativas de colaboradores desligados, de severidade alta, com revisão imediata dos acessos.

7.2. Compete à equipe de Risco e Compliance a comunicação da contingência aos demais colaboradores, orientando-os sobre a postura e as providências cabíveis, em observância ao Plano de Continuidade de Negócios.

7.3. Cabe à equipe de Risco e Compliance elaborar relatórios acerca dos danos ocorridos, do percentual das atividades afetadas e dos impactos financeiros, sugerindo as medidas necessárias ao retorno à normalidade, submetendo-os à Diretoria.

7.4. Sempre que o incidente cibernético envolver dados pessoais, o Diretor de Risco, Compliance e PLD observará, adicionalmente, o procedimento e os prazos previstos nos itens 3.13 e 3.14.

7.5. Após o retorno à normalidade, a Sociedade estudará procedimentos preventivos a serem implementados e incluídos no Plano de Continuidade de Negócios.

CAPÍTULO VIII

Programa de Treinamento

8.1. A Sociedade conta com programa de treinamento periódico dos colaboradores que tenham acesso a informações confidenciais, na forma descrita no Código de Ética e Conduta. O treinamento aborda o tratamento das informações confidenciais e, quanto aos dados pessoais, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e os benefícios decorrentes do tratamento.

8.2. Os procedimentos e rotinas definidos nesta Política são abordados em treinamento anual, coordenado pelo Diretor de Risco, Compliance e PLD ou por terceiro contratado para esse fim, estendido aos terceiros contratados relevantes.

8.3. Poderão ser promovidos treinamentos extraordinários em periodicidade menor, em especial em virtude de mudanças relevantes nos procedimentos e controles descritos nesta Política.

CAPÍTULO IX

Disposições Gerais, Aprovação e Vigência

9.1. Todos os documentos, relatórios e informações relevantes para os procedimentos e rotinas descritos nesta Política são arquivados em meio físico ou eletrônico pelo prazo mínimo de 5 (cinco) anos.

9.2. A aprovação desta Política e de suas revisões compete ao Diretor de Gestão, em conjunto com o Diretor de Risco, Compliance e PLD. Esta Política entra em vigor na data de sua aprovação, aplicando-se os controles e registros nela previstos aos eventos ocorridos a partir dessa data.

9.3. Esta Política será revisada no mínimo anualmente, ou em prazo inferior sempre que houver alteração relevante na regulação em vigor, nas regras de autorregulação, na estrutura, nas atividades ou nos sistemas da Sociedade, mantido o controle de versões.

9.4. O presente instrumento prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os colaboradores aos seus termos e condições.

9.5. A título de enforcement, a não observância dos dispositivos desta Política resultará em advertência, suspensão, demissão ou exclusão por justa causa, conforme a gravidade e a reincidência da violação, na forma do Capítulo XI do Código de Ética e Conduta, sem prejuízo das penalidades civis e criminais aplicáveis.