POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CIBERSEGURANÇA E PROTEÇÃO DE DADOS PESSOAIS

ABRIL 2025

Sumário

1. INTRODUÇÃO E OBJETIVO

A presente Política de Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais ("Política") tem por objetivo estabelecer os princípios, critérios e procedimentos adotados pela B6 CAPITAL GESTORA DE RECURSOS LTDA. ("Gestora") para assegurar a confidencialidade, integridade, disponibilidade e privacidade das informações de propriedade da Gestora, bem como dos dados pessoais de clientes, cotistas, investidores, colaboradores e demais partes relacionadas.

Esta Política foi elaborada em conformidade com a Resolução da Comissão de Valores Mobiliários ("CVM") nº 50, de 31 de agosto de 2021 ("Resolução CVM nº 50"), com o Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA de Administração de Recursos de Terceiros ("Código ANBIMA"), com o Guia de Cibersegurança da ANBIMA, bem como com a Lei nº 13.709, de 14 de agosto de 2018, de Proteção de Dados Pessoais ("LGPD") e demais normas aplicáveis.

Adicionalmente, esta Política se aplica compulsoriamente a todos os Colaboradores da Gestora, sócios e prestadores de serviços que, no âmbito de suas atividades, tenham acesso a informações confidenciais ou dados pessoais tratados pela Gestora.

2. APLICAÇÃO E RESPONSABILIDADES

A presente Política se aplica a todos os Colaboradores da Gestora, sócios e prestadores de serviços que, no exercício de suas funções, tenham acesso ou contato com informações confidenciais, dados pessoais ou sistemas críticos da Gestora.

2.1. DIRETOR DE *COMPLIANCE*, RISCO E PLD

É responsabilidade do Diretor de *Compliance*, Risco e PLD:

(i) Coordenar a implementação, o monitoramento e a atualização desta Política;

(ii) Avaliar e definir as estratégias de segurança da informação, cibersegurança e proteção de dados pessoais da Gestora;

(iii) Realizar testes periódicos e promover treinamentos aos Colaboradores, conforme previsto nesta Política;

(iv) Analisar e reportar eventuais incidentes de segurança às autoridades competentes, quando aplicável;

(v) Assegurar a conformidade com a legislação e regulamentação vigente, incluindo a Resolução CVM nº 50/2021, o Código ANBIMA de Administração de Recursos de Terceiros e a Lei Geral de Proteção de Dados (LGPD).

2.2. COLABORADORES, SÓCIOS E PRESTADORES DE SERVIÇOS

São responsabilidades dos Colaboradores, Sócios e Prestadores de Serviços:

(i) Cumprir integralmente as disposições desta Política e demais normas internas

relacionadas à segurança da informação, cibersegurança e proteção de dados pessoais;

(ii) Utilizar os sistemas, redes e informações da Gestora exclusivamente para fins profissionais, respeitando as práticas de segurança estabelecidas;

(iii) Proteger as informações confidenciais e os dados pessoais a que tiverem acesso, abstendo-se de divulgá-los a terceiros não autorizados;

(iv) Reportar imediatamente ao Diretor de *Compliance*, Risco e PLD qualquer incidente de segurança, violação ou suspeita de violação de dados;

(v) Participar dos treinamentos e programas de conscientização promovidos pela Gestora.

3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO E DE PROTEÇÃO DE DADOS

A atuação da Gestora em matéria de segurança da informação, cibersegurança e proteção de dados pessoais é orientada pelos seguintes princípios:

3.1. CONFIDENCIALIDADE

As informações sob gestão da Gestora devem ser protegidas contra o acesso não autorizado. O acesso é restrito exclusivamente às pessoas que necessitem das informações para o desempenho de suas funções profissionais, no limite de sua necessidade e competência.

3.2. INTEGRIDADE

As informações devem ser mantidas em seu estado original, de modo a preservar a sua exatidão, consistência e confiabilidade, sendo vedadas alterações indevidas, acidentais ou intencionais.

3.3. DISPONIBILIDADE

As informações devem estar acessíveis e utilizáveis quando necessário, garantindo a continuidade das operações e o desempenho das atividades da Gestora.

3.4. PRIVACIDADE DE DADOS PESSOAIS

O tratamento de dados pessoais, incluindo dados sensíveis, será realizado em conformidade com a legislação aplicável, especialmente a LGPD, respeitando os direitos dos titulares e assegurando a sua finalidade legítima, necessidade, adequação, livre acesso, qualidade, transparência, segurança, prevenção e responsabilidade.

4. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS (RISK ASSESSMENT)

No âmbito de suas atividades, a Gestora realiza a identificação e a avaliação contínua dos principais riscos relacionados à segurança da informação, à cibersegurança e à proteção de dados pessoais. Foram identificados os seguintes riscos internos e externos que demandam proteção:

(i) **Dados e Informações**: riscos relacionados às Informações Confidenciais, incluindo dados de investidores, clientes, Colaboradores e da própria Gestora, bem

como às operações e ativos investidos pelas carteiras sob gestão e às comunicações internas e externas;

(ii) **Sistemas**: riscos relacionados às informações sobre os sistemas utilizados pela Gestora e às tecnologias desenvolvidas internamente ou por terceiros, incluindo ameaças possíveis e vulnerabilidades;

(iii) **Processos e Controles**: riscos envolvendo processos e controles internos que são parte da rotina das áreas de negócios da Gestora;

(iv) **Governança da Gestão de Risco**: riscos quanto à eficácia dos processos de gestão de risco da Gestora, abrangendo ameaças, planos de ação, contingência e continuidade de negócios.

No que se refere especificamente à segurança cibernética, a Gestora reconhece as seguintes ameaças principais, conforme previsto no Guia de Cibersegurança da ANBIMA:

(i) **Malware**: softwares maliciosos que visam corromper computadores e redes, incluindo vírus, cavalos de troia, spyware e ransomware;

(ii) **Engenharia Social**: métodos de manipulação para obtenção de informações confidenciais, tais como pharming, phishing, vishing, smishing e acesso pessoal;

(iii) **Ataques de DDoS (Distributed Denial of Service) e botnets**: ataques que visam negar ou atrasar o acesso a serviços ou sistemas da Gestora;

(iv) **Invasões (Advanced Persistent Threats)**: ataques realizados por agentes sofisticados que detectam e exploram fragilidades específicas em ambientes tecnológicos.

Com base na avaliação desses riscos, a Gestora define e implementa um plano estratégico de prevenção, mitigação e acompanhamento, contemplando, quando necessário, a adoção de modificações, planos de contingência e planos de retomada das atividades normais e de restabelecimento da segurança devida.

5. MEDIDAS DE PREVENÇÃO E PROTEÇÃO

5.1. REGRA GERAL DE CONDUTA

A Gestora realiza efetivo controle do acesso a arquivos que contenham Informações Confidenciais, disponibilizando-os somente aos Colaboradores diretamente envolvidos no projeto que demanda seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam arquivos utilizados, gerados ou disponíveis na rede da Gestora, e circulem em ambientes externos com tais documentos, salvo se em prol da execução e desenvolvimento dos negócios e interesses da Gestora. Nesse caso, o Colaborador é o responsável direto pela boa conservação, integridade e manutenção da confidencialidade da informação.

A troca de informações entre os Colaboradores deve se pautar no conceito da necessidade

de conhecimento, sendo que, em caso de dúvida quanto à pertinência do compartilhamento, a Equipe de Compliance e Risco deve ser previamente acionada. Documentos contendo Informações Confidenciais não devem ser deixados expostos nas estações de trabalho ou em outros espaços da Gestora durante a ausência do usuário, especialmente após o expediente. Discussões e acessos remotos a Informações Confidenciais são expressamente proibidos.

Qualquer impressão de documentos deve ser retirada imediatamente da impressora, sendo vedado o abandono de documentos impressos. A Gestora não mantém arquivo físico centralizado, cabendo a cada Colaborador a responsabilidade pela conservação, integridade e segurança das informações sob sua guarda. O descarte de informações confidenciais deve ser feito de forma segura, utilizando-se trituração para documentos físicos e procedimentos que impeçam a recuperação de arquivos digitais.

O uso de dispositivos como pen-drives, fitas ou discos é restrito à finalidade exclusiva de desempenho das atividades profissionais. É vedado o envio ou repasse de material discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo por e-mail, bem como de mensagens que possam afetar a imagem ou reputação da Gestora. Mensagens recebidas com tais características devem ser apagadas imediatamente. A navegação em sites de conteúdo discriminatório, ofensivo ou impróprio é proibida.

5.2. CONTROLE DE ACESSOS FÍSICOS E LÓGICOS

A Gestora mantém níveis diferenciados de acesso às pastas e arquivos eletrônicos, atribuídos de acordo com a função e senioridade dos Colaboradores, por meio de login e senha individuais. Tais mecanismos visam limitar a exposição e a vulnerabilidade dos sistemas em caso de violação.

O acesso de pessoas externas a áreas restritas da Gestora só é permitido mediante autorização expressa de Colaboradores autorizados. A utilização de equipamentos e sistemas é monitorada para assegurar que sejam utilizados exclusivamente para fins profissionais.

5.3. SENHA E LOGIN

As senhas e logins para acesso aos computadores e sistemas da Gestora são pessoais e intransferíveis, devendo ser conhecidas apenas pelo usuário autorizado. As senhas devem ser trocadas periodicamente, preferencialmente a cada seis meses, conforme aviso da área responsável pela tecnologia da informação.

Colaboradores que disponibilizarem suas credenciais de acesso a terceiros responderão pelas consequências decorrentes de tal prática, inclusive quanto a incidentes de segurança.

5.4. USO DE EQUIPAMENTOS E SISTEMAS

Cada Colaborador é responsável pela segurança das informações armazenadas nos

equipamentos sob sua responsabilidade. A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet e e-mails, destina-se prioritariamente ao exercício de atividades profissionais. O uso pessoal deve ser restrito e nunca prejudicar as atividades da Gestora. O uso indevido ou inadequado de qualquer ativo deve ser reportado imediatamente à Equipe de *Compliance* e Risco.

5.5. ACESSO REMOTO

O acesso remoto aos sistemas da Gestora é permitido a todos os Colaboradores, mediante utilização de credenciais individuais de acesso (login e senha), respeitadas as políticas internas de segurança da informação.

O acesso a e-mails corporativos, documentos e sistemas pode ser realizado a partir de dispositivos pessoais dos Colaboradores, desde que esses dispositivos estejam protegidos por senha de acesso e contem com softwares atualizados de proteção contra malwares.

Os Colaboradores devem zelar pela confidencialidade e integridade das informações acessadas remotamente, devendo comunicar imediatamente à Equipe de Compliance e Risco qualquer violação ou ameaça de segurança cibernética identificada durante a realização de suas atividades.

É vedado o armazenamento permanente de Informações Confidenciais da Gestora em dispositivos pessoais. O acesso e o uso das informações devem se restringir à finalidade estritamente profissional, respeitando os limites de segurança estabelecidos nesta Política.

5.6. FIREWALL, SOFTWARE, VARREDURAS E BACKUP

A Gestora utiliza firewall dedicado para proteção contra conexões não autorizadas e incursões maliciosas. A proteção contra malware é assegurada por meio de sistemas de antivírus atualizados em todos os dispositivos. São realizadas varreduras periódicas, ao menos anuais, para detecção de programas maliciosos, além da implementação de patches de segurança nos sistemas conforme definido pelo Diretor de *Compliance*, Risco e PLD.

As informações da Gestora são objeto de backup automático em ambiente seguro na nuvem, sendo esses procedimentos testados regularmente para garantir a sua eficácia e disponibilidade em caso de incidentes.

6. MONITORAMENTO E TESTES DE SEGURANÇA

A Gestora realiza o monitoramento periódico dos seus ambientes de tecnologia e das práticas de segurança da informação adotadas, visando assegurar a proteção contínua de seus dados, sistemas e ativos.

O monitoramento inclui a verificação do uso adequado dos ativos tecnológicos pelos

Colaboradores, a análise de acessos realizados aos sistemas e a supervisão do tráfego de informações armazenadas ou transmitidas nos ambientes da Gestora. Eventuais inconformidades ou suspeitas de incidentes de segurança devem ser reportadas imediatamente à Equipe de Compliance e Risco.

A Gestora promove testes periódicos de segurança em seus sistemas e dispositivos, incluindo varreduras de proteção contra malwares, atualização de patches de segurança e verificação de integridade de backups. As varreduras de segurança têm periodicidade mínima anual ou sempre que identificada alguma situação de risco que exija medida corretiva.

Esses procedimentos visam identificar possíveis vulnerabilidades e assegurar a eficácia das medidas preventivas e corretivas implementadas, contribuindo para a continuidade e a resiliência operacional da Gestora.

A Equipe de *Compliance* e Risco é responsável pela coordenação das atividades de monitoramento e testes de segurança, devendo manter registros apropriados das verificações realizadas e propor, sempre que necessário, melhorias ou atualizações dos controles internos.

7. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA E VAZAMENTOS DE DADOS

A Gestora adota procedimentos para a identificação, comunicação e tratamento de incidentes de segurança da informação e vazamentos de dados pessoais. Qualquer suspeita ou confirmação de incidente, incluindo acessos não autorizados, falhas de segurança, perda, destruição ou divulgação indevida de informações ou dados pessoais, deve ser comunicada imediatamente à Equipe de *Compliance* e Risco.

Recebida a comunicação, a Equipe avaliará o tipo e a gravidade do incidente, considerando a natureza das informações afetadas, a extensão do impacto e as medidas corretivas cabíveis. Sempre que necessário, serão tomadas providências para conter o incidente, recuperar as informações afetadas, e minimizar danos.

Nos casos que envolvam dados pessoais, a Gestora avaliará, conforme a legislação aplicável, a necessidade de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e, se for o caso, aos titulares dos dados afetados.

O tratamento dos incidentes será documentado, incluindo a descrição do evento, a análise das causas, as medidas adotadas e as recomendações para evitar recorrências. A Equipe de *Compliance* e Risco é responsável pela coordenação das ações de resposta e pela definição das comunicações internas e externas necessárias, de acordo com a legislação e as boas práticas de mercado.

Para fins de governança e conformidade regulatória, todos os registros relacionados à

identificação, análise e tratamento de incidentes de segurança da informação e vazamentos de dados serão devidamente documentados e arquivados pela Gestora pelo prazo mínimo de cinco anos, em conformidade com as disposições da regulamentação aplicável e com as práticas de controle interno estabelecidas no Manual de Compliance e Controles Internos da instituição.

8. TRATAMENTO DE DADOS PESSOAIS E DIREITOS DOS TITULARES

A Gestora realiza o tratamento de dados pessoais no estrito cumprimento da legislação aplicável, em especial da LGPD. O tratamento de dados pessoais é realizado de forma adequada, limitada às finalidades legítimas vinculadas à gestão de investimentos, à execução de contratos, ao cumprimento de obrigações legais ou regulatórias e à proteção do exercício regular de direitos da Gestora.

Para proteção contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão indevida, a Gestora adota medidas técnicas e administrativas adequadas, incluindo procedimentos de segurança da informação e de controle de acesso.

Em conformidade com a LGPD, os titulares de dados pessoais tratados pela Gestora têm direito, mediante requisição formal, a obter:

(i) A confirmação da existência de tratamento de seus dados pessoais;
(ii) O acesso aos dados tratados;
(iii) A correção de dados incompletos, inexatos ou desatualizados;
(iv) A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação;
(v) A portabilidade dos dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial;
(vi) A eliminação dos dados pessoais tratados com base no consentimento, nos termos da legislação aplicável;
(vii) A informação sobre as entidades públicas e privadas com as quais seus dados foram compartilhados;
(viii) A informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
(ix) A revogação do consentimento, quando aplicável.

O atendimento às solicitações dos titulares será realizado pela Equipe de *Compliance* e Risco, observadas as disposições legais, a viabilidade técnica e a proteção de informações confidenciais da Gestora ou de terceiros.

9. CONFIDENCIALIDADE E USO DE INFORMAÇÕES

Todas as informações a que os Colaboradores, Sócios e Prestadores de Serviços da Gestora tenham acesso em razão de suas atividades são consideradas confidenciais,

independentemente da forma de acesso, armazenamento ou transmissão.

São consideradas **Informações Confidenciais** todas as informações que, por sua natureza, não sejam públicas, incluindo, mas não se limitando a: dados pessoais de clientes, investidores, fornecedores, prestadores de serviços e Colaboradores; informações sobre estratégias de investimento, estrutura de produtos, carteiras sob gestão, operações realizadas, políticas internas, práticas comerciais, metodologias de trabalho, contratos, correspondências internas e externas, relatórios, estudos técnicos e quaisquer outras informações estratégicas ou sensíveis relativas à Gestora ou a terceiros com quem esta mantenha relacionamento.

O compromisso de confidencialidade abrange o dever de proteger as Informações Confidenciais contra acesso, divulgação, modificação, uso ou destruição não autorizados, bem como a obrigação de utilizar tais informações exclusivamente para os fins relacionados às atividades profissionais exercidas no âmbito da Gestora.

É vedado divulgar, reproduzir, armazenar em mídias não autorizadas, compartilhar com terceiros não autorizados ou utilizar Informações Confidenciais para benefício próprio ou de terceiros. A responsabilidade pela guarda e proteção das Informações Confidenciais é individual e direta de cada Colaborador, Sócio ou Prestador de Serviços que tenha acesso a tais dados.

No caso de término do vínculo com a Gestora, por qualquer motivo, o compromisso de confidencialidade permanecerá vigente, obrigando o ex-Colaborador, ex-Sócio ou ex-Prestador de Serviços a manter o sigilo e a não utilizar ou divulgar quaisquer informações obtidas em razão de sua atuação.

Para reforçar o compromisso com a proteção das Informações Confidenciais, todos os Colaboradores devem assinar o Termo de Adesão à Cláusula de Propriedade Intelectual e Confidencialidade, constante no Anexo II do Manual de Compliance e Controles Internos. Ao assiná-lo, comprometem-se a respeitar os direitos da Gestora sobre ativos intangíveis e a manter o sigilo das informações acessadas, inclusive após o término do vínculo.

A violação às regras de confidencialidade poderá ensejar a aplicação das penalidades cabíveis, sem prejuízo das responsabilidades civis e criminais aplicáveis.

9.1. PROPRIEDADE INTELECTUAL

Todos os materiais, documentos, modelos, processos, metodologias, conteúdos e demais ativos intangíveis desenvolvidos ou utilizados no âmbito das atividades da Gestora são considerados propriedade intelectual da mesma, conforme regulamentação vigente e as diretrizes internas.

O compromisso de preservação da propriedade intelectual é formalizado pelos

Colaboradores mediante a assinatura do Termo de Adesão à Cláusula de Propriedade Intelectual e Confidencialidade, constante do Manual de Compliance e Controles Internos da Gestora. Tal Termo estabelece a obrigação de respeitar integralmente os direitos da Gestora sobre seus ativos intangíveis e de manter a confidencialidade das informações obtidas em razão do vínculo funcional ou contratual, inclusive após seu encerramento.

10. TREINAMENTO E CONSCIENTIZAÇÃO

A Gestora reconhece que a eficácia das práticas de segurança da informação, cibersegurança e proteção de dados pessoais depende da conscientização e do comprometimento de todos os seus Colaboradores.

Com o objetivo de fomentar a cultura de segurança e de garantir a adequada compreensão das normas e procedimentos previstos nesta Política, a Gestora promove treinamentos periódicos voltados aos temas de segurança da informação, proteção de dados pessoais e boas práticas de uso de sistemas e ativos tecnológicos.

Os treinamentos são direcionados a todos os Colaboradores, abrangendo tanto os profissionais recém-admitidos quanto os já integrados ao quadro da Gestora, com atualização sempre que houver alteração relevante nas políticas internas ou nas normas legais e regulamentares aplicáveis.

Além dos treinamentos formais, a Gestora realiza ações de conscientização destinadas a reforçar as orientações sobre a importância da proteção de informações confidenciais e do correto tratamento de dados pessoais.

A participação nos treinamentos e programas de conscientização é obrigatória, cabendo à Equipe de *Compliance* e Risco a coordenação, registro e controle de presença dos Colaboradores.

11. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada **anualmente**, podendo ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

HISTÓRICO DE ATUALIZAÇÕES		
Data	**Versão**	**Responsável**
Novembro de 2023	1ª	Diretor de *Compliance*, Risco e PLD
Novembro de 2024	2ª	Diretor de *Compliance*, Risco e PLD
Abril de 2025	3ª e atual	Diretor de *Compliance*, Risco e PLD