

ATOL CAPITAL GESTORA DE RECURSOS LTDA.

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

AGOSTO / 2026

HISTÓRICO DE ALTERAÇÕES

Versão	Data	Modificado Por	Resumo da Alteração
1.0	Agosto/2026	Tamarin Consultoria	Versão Inicial

ÍNDICE

OBJETIVO.....	3
CONFIDENCIALIDADE E ACESSOS.....	4
AMEAÇAS CIBERNÉTICAS.....	4
CLASSIFICAÇÃO DE CRITICIDADE DAS INFORMAÇÕES.....	5
ESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO.....	7
Estrutura Geral de Informática.....	7
Regras Gerais, Acessos e Senhas.....	8
<i>Softwares e sistemas</i>	9
Registros.....	9
Responsabilidades do usuário.....	10
Proteções Adicionais aos Notebooks.....	11
Regras e responsabilidades do uso da Internet.....	11
Uso de correio eletrônico.....	12
Programas de comunicação corporativa.....	13
TREINAMENTO E CONSCIENTIZAÇÃO.....	13
MONITORAMENTO E TESTES PERIÓDICOS.....	14
PLANO DE RESPOSTA.....	14
PROTEÇÃO DE DADOS PESSOAIS.....	16
DISPOSIÇÕES GERAIS.....	21
ANEXO I.....	22

OBJETIVO

A Política de Proteção de Dados, Segurança da Informação e Cibernética (“Política”) da Atol Capital Gestora de Recursos Ltda. (“Atol Capital” ou “Gestora”), estabelece os procedimentos e controles adotados para assegurar a confidencialidade, integridade e disponibilidade das informações, dados e sistemas utilizados no âmbito de suas atividades.

A presente Política aplica-se a todos os sócios, funcionários, analistas, colaboradores (“Colaboradores”) e prestadores de serviços relevantes, cabendo a todos os usuários de recursos tecnológicos a responsabilidade pela proteção das informações, sistemas e equipamentos da Gestora. Os prestadores de serviços que tiverem acesso a Informações Confidenciais deverão firmar termo de confidencialidade ou estar sujeitos a cláusula contratual equivalente, e as obrigações de confidencialidade previstas nesta Política permanecerão em vigor após o encerramento do vínculo do Colaborador ou do prestador de serviços com a Gestora, enquanto as respectivas informações não se tornarem públicas.

Em conformidade com a regulamentação aplicável, incluindo a Resolução nº 21/2021 da Comissão de Valores Mobiliários (“CVM”), as Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (“ANBIMA”), o Guia de Cibersegurança da ANBIMA, a Resolução CVM nº 50/2021 e a Lei nº 13.709/2018 (“LGPD”) e a regulamentação da Autoridade Nacional de Proteção de Dados (“ANPD”), a Gestora adota medidas destinadas à identificação e mitigação de riscos, especialmente em relação a informações sensíveis e eventos que possam impactar suas atividades.

As Informações Confidenciais obtidas no exercício das atividades da Gestora somente poderão ser divulgadas mediante autorização prévia do Diretor de Risco, Compliance e PLD e em observância à regulamentação aplicável, sendo vedado seu compartilhamento com pessoas que não necessitem de acesso para o desempenho de suas funções. Independem da referida autorização (i) o compartilhamento, no curso regular das atividades, com prestadores de serviços dos fundos e carteiras geridos (administrador fiduciário, custodiante, corretoras, distribuidores e auditores) sujeitos a dever de sigilo; e (ii) o atendimento a exigências de autoridades reguladoras e autorreguladoras, observado o disposto na seção “Cooperação com Autoridades”.

Qualquer requisição, intimação ou ordem de autoridade judicial, administrativa, reguladora ou autorreguladora que envolva Informações Confidenciais, recebida por qualquer Colaborador, deverá ser encaminhada imediata e previamente ao Diretor de Risco, Compliance e PLD, a quem caberá definir a forma e o conteúdo da resposta, observado o dever de colaboração da Gestora com as autoridades competentes.

Consideram-se “Informações Confidenciais” todo e qualquer dado, em qualquer formato ou meio, relacionado às atividades da Atol Capital, incluindo, mas não se limitando a *know-how*, informações

técnicas, financeiras, comerciais e estratégicas, posições e operações de clientes e fundos, bem como dados sobre sócios, colaboradores, clientes, contrapartes e prestadores de serviços, obtidos em razão do desempenho das atividades do Colaborador ou do relacionamento com a Gestora e seus parceiros. Incluem-se, ainda, as informações privilegiadas, assim entendidas as informações relevantes ainda não divulgadas ao mercado, nos termos da Resolução CVM nº 44/2021, cujo tratamento observará também o Manual de Ética e Controles Internos e as demais políticas internas da Gestora.

O Colaborador que tiver acesso, por qualquer meio, inclusive acidental, a Informação Confidencial ou privilegiada à qual não deveria ter acesso deverá comunicar imediatamente o fato ao Diretor de Risco, Compliance e PLD, indicando a respectiva fonte, e abster-se de utilizá-la ou transmiti-la a terceiros. Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para negociação de valores mobiliários, em nome próprio ou de terceiros, ou para a prática de *insider trading*, *front-running* ou transmissão de dicas, sujeitando-se o infrator às sanções previstas nas políticas internas da Gestora e na legislação aplicável.

CONFIDENCIALIDADE E ACESSOS

Os Colaboradores da Atol Capital utilizam *notebooks* de uso individual, protegidos por credenciais de acesso (*login* e senha) próprias e intransferíveis. Cada Colaborador possui equipamento e credenciais individualizadas, sendo vedado o compartilhamento de acessos.

O acesso às informações e sistemas da Gestora é restrito aos Colaboradores que necessitem de tais acessos para o desempenho de suas funções, observando-se a segregação de pastas, arquivos e sistemas entre as diferentes áreas e usuários.

Os acessos às informações, sistemas e pastas da Atol Capital são controlados pelo Diretor de Risco, Compliance e PLD, a quem compete supervisionar e monitorar a adequada segregação de acessos em todas as áreas da Gestora. No âmbito da Área de Gestão, cabe ao Diretor de Gestão definir os níveis de acesso dos Colaboradores às pastas, sistemas e informações sob sua responsabilidade, observadas as diretrizes estabelecidas pelo Diretor de Risco, Compliance e PLD, que detém a supervisão geral sobre a segregação de informações e acessos. Nas ausências e impedimentos do Diretor de Risco, Compliance e PLD, tais atribuições serão exercidas por substituto por ele designado que não integre a Área de Gestão, sendo mantida credencial administrativa de contingência, sob guarda da Diretoria, para acesso emergencial aos ambientes corporativos.

AMEAÇAS CIBERNÉTICAS

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, nível de informações ou característica dos ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos ser irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- a) Malware (*Bots*, Cavalo de Tróia, *Ransomware*, *Spyware*, Vírus e *Worms*): *Software* malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de *software* costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites.
- b) Engenharia Social (*Clickjacking*, *Deepfake*, Espionagem Cibernética, *Phishing*, *quishing*, *Smishing*, *Spoofing* e *Vishing*): Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da segurança da informação, é considerada uma prática de má-fé para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de indivíduos, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes.
- c) Ataques de DoS (Negação de Serviços), DDoS (Negação de Serviço Distribuída) e botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da organização, no caso das *botnets*, o ataque vem de muitos computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- d) Intrusões (Ataque de força bruta e MitM – *Man in the Middle*): Ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.
- e) Fraude por comprometimento de e-mail e instruções fraudulentas (*Business Email Compromise* – BEC): Solicitações de pagamento, resgate, alteração de dados bancários ou cadastrais, ou transmissão de ordens, aparentemente emitidas por Colaboradores, clientes, administrador fiduciário ou contrapartes, inclusive com uso de *deepfake* de voz ou vídeo, com o objetivo de desviar recursos ou obter Informações Confidenciais.

Ainda, além de ataques cibernéticos, a Atol Capital pode estar sujeita a mau funcionamento dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar a perda e/ou adulteração de dados e Informações Confidenciais.

CLASSIFICAÇÃO DE CRITICIDADE DAS INFORMAÇÕES

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para a Gestora, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para a Atol Capital, em caso de incidente de segurança.

Deste modo, a Gestora segrega as informações geradas pela instituição, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classificam-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

Baixo Risco

- a) Quaisquer informações e/ou dados que a Gestora teve acesso ou conhecimento por ser de domínio público (“Informação Pública”);
- b) Quaisquer informações e/ou dados que não estejam sujeitos a compromissos ou acordos de confidencialidade; ou
- c) Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente (e.g., cota e patrimônio líquido dos fundos).

Médio Risco

- a) Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas ainda não foram entregues (Ex: Formulário de Referência).
- b) Informações encaminhadas a investidores, alocadores e parceiros sob compromisso de confidencialidade, tais como questionários de due diligence (DDQ), apresentações institucionais e relatórios de gestão, bem como a composição da carteira dos fundos cuja divulgação seja admitida com defasagem pela regulamentação aplicável, enquanto não decorrido o respectivo prazo.

Alto Risco

- a) Todas as Informações Confidenciais, incluindo:
 - *Know-how*, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela Atol Capital;
 - Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Atol Capital;
 - Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e/ou de seus sócios e clientes; e

- Informações relativas a denúncias, potenciais conflitos de interesse, investigações internas e relatórios de Compliance, cujo acesso é restrito à Área de Risco, Compliance e PLD e à Diretoria.

A partir da definição acima, a Atol Capital se empenhará em manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: Alto Risco, Médio Risco e Baixo Risco.

Para cada classe, a Gestora observará os seguintes controles mínimos: (i) Alto Risco: armazenamento exclusivamente no ambiente corporativo, acesso restrito por necessidade de conhecimento, transmissão apenas por correio eletrônico corporativo ou compartilhamento com controle de acesso, vedado o armazenamento em contas pessoais e a circulação por aplicativos de mensagens instantâneas, e descarte seguro (fragmentação de documentos físicos e exclusão definitiva de arquivos eletrônicos); (ii) Médio Risco: armazenamento no ambiente corporativo e divulgação restrita até a data de publicação; e (iii) Baixo Risco: sem restrições específicas.

ESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO

Estrutura Geral de Informática

A Atol Capital utiliza infraestrutura tecnológica baseada em sistemas em nuvem fornecidos por prestadores de serviços reconhecidos, incluindo Google, Microsoft e Apple, permitindo o acesso seguro, remoto e contínuo às informações e sistemas corporativos da Gestora.

Nesse contexto, a Gestora disponibiliza aos Colaboradores acesso ao pacote corporativo Microsoft Office 365, incluindo SharePoint, que constitui o repositório oficial das informações da Gestora, sendo vedado o armazenamento de Informações Confidenciais em contas pessoais de armazenamento em nuvem (tais como Google Drive ou iCloud pessoais), observadas as diretrizes de segregação de acessos e confidencialidade estabelecidas nesta Política.

As informações mantidas no ambiente Microsoft 365 (correio eletrônico, SharePoint e OneDrive) serão objeto de rotina de backup independente dos recursos nativos de retenção do provedor, com periodicidade mínima diária e retenção compatível com o prazo de guarda de 5 (cinco) anos previsto na regulamentação aplicável, sendo a restauração testada ao menos anualmente.

No processo de aprovação do equipamento, deverá ser verificado se este (i) possui capacidade operacional compatível com os *softwares* e aplicações necessários ao desempenho das atividades do Colaborador; (ii) conta com sistema operacional atualizado e apto à utilização segura dos recursos tecnológicos da Gestora; (iii) possui mecanismos de proteção ativos, incluindo antivírus nativo em funcionamento contínuo, com realização periódica de varreduras e monitoramento de potenciais ameaças cibernéticas; (iv) possui criptografia integral de disco ativada (e.g., FileVault ou BitLocker); e

(v) está inscrito na ferramenta de gestão de dispositivos adotada pela Gestora, que permita a verificação periódica dos requisitos acima e o apagamento remoto das informações corporativas em caso de perda, furto ou desligamento do Colaborador.

Essa estrutura possibilita a execução das atividades da Gestora de forma segura e contínua, independentemente do local de acesso dos Colaboradores, em linha com as diretrizes estabelecidas no Plano de Continuidade de Negócios da Atol Capital.

A contratação de prestadores de serviços de processamento e armazenamento de dados e de computação em nuvem será precedida de diligência proporcional à relevância do serviço, preferencialmente com base no Questionário ANBIMA de Due Diligence para Contratação de Terceiros e Serviços em Nuvem, devendo os respectivos contratos ou termos de serviço contemplar obrigações de confidencialidade, segurança da informação, comunicação de incidentes e proteção de dados pessoais, nos termos do art. 39 da LGPD.

O acesso físico às dependências da Gestora é restrito aos Colaboradores, devendo visitantes permanecer acompanhados. Documentos físicos que contenham Informações Confidenciais deverão ser mantidos em local trancado quando não estiverem em uso, a impressão deverá limitar-se ao estritamente necessário e o descarte deverá ser realizado por fragmentação ou processo equivalente que impeça sua recuperação. A perda de qualquer documento ou equipamento que contenha Informações Confidenciais deverá ser comunicada imediatamente ao Diretor de Risco, Compliance e PLD.

Regras Gerais, Acessos e Senhas

O uso dos recursos tecnológicos da Atol Capital pelos Colaboradores deve respeitar as seguintes regras:

- a) O acesso aos sistemas e plataformas corporativas da Atol Capital será realizado mediante utilização de credenciais individuais e intransferíveis;
- b) A criação, alteração e exclusão de usuários e acessos aos sistemas e contas corporativas são realizadas mediante autorização do Diretor de Risco, Compliance e PLD;
- c) As senhas devem observar requisitos mínimos de segurança, incluindo comprimento mínimo de 12 (doze) caracteres, padrão de complexidade (caracteres alfanuméricos, maiúsculos e minúsculos) e renovação periódica em prazo não superior a 180 (cento e oitenta) dias;
- d) É obrigatória a autenticação multifator (MFA) para acesso ao correio eletrônico corporativo, ao ambiente Microsoft 365, aos portais de administradores fiduciários, custodiantes e corretoras e a quaisquer sistemas que contenham Informações Confidenciais; nos demais sistemas, sempre que disponível, os acessos deverão contar com mecanismos adicionais de autenticação, incluindo MFA e/ou *Single Sign-On* (SSO);

- e) Os acessos são individuais, rastreáveis e auditáveis, sendo vedada a utilização de credenciais compartilhadas ou padronizadas entre sistemas;
- f) Os acessos concedidos serão revisados, no mínimo, semestralmente pela Área de Risco, Compliance e PLD, com a revogação daqueles que não mais se justifiquem; e
- g) No desligamento do Colaborador, todos os seus acessos serão revogados em até 24 (vinte e quatro) horas, devendo as Informações Confidenciais armazenadas em equipamentos pessoais ser devolvidas e eliminadas, com verificação pela Área de Risco, Compliance e PLD, e o correio eletrônico corporativo ser preservado pelo prazo de guarda aplicável.

Softwares e sistemas

A utilização, instalação e acesso a sistemas, *softwares* e aplicações no ambiente tecnológico da Atol Capital estão sujeitos aos seguintes controles:

- a) Todos os *softwares* e sistemas utilizados pelos Colaboradores para o exercício de suas funções na Gestora devem ser previamente aprovados pela Área de Risco, Compliance e PLD, sendo vedada a instalação ou utilização de ferramentas não autorizadas;
- b) O acesso aos sistemas e plataformas é concedido de forma individualizada, conforme a necessidade do Colaborador para o desempenho de suas funções, observada a segregação de acessos;
- c) As permissões de acesso e poderes outorgados aos Colaboradores são definidas de acordo com as atribuições do Colaborador, sob avaliação do Diretor de Gestão e/ou do Diretor de Risco, Compliance e PLD, conforme aplicável;
- d) A utilização de equipamentos pessoais por terceiros nos ambientes tecnológicos da Atol Capital e a conexão destes à rede interna da Gestora requerem autorização prévia e expressa do Diretor de Risco, Compliance e PLD. Os Colaboradores estão autorizados a conectar seus telefones celulares e *notebooks* pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais corporativas de acesso;
- e) A conexão de dispositivos móveis de armazenamento (e.g. *USB Drive*) somente poderá ser realizada mediante autorização prévia e expressa do Diretor de Risco, Compliance e PLD.

A Área de Risco, Compliance e PLD manterá inventário atualizado dos sistemas, softwares, contas corporativas, equipamentos aprovados e prestadores de serviços de tecnologia utilizados pela Gestora, o qual servirá de base para a identificação e avaliação de riscos cibernéticos e para os testes periódicos previstos nesta Política.

Registros

A Atol Capital utiliza sistemas e plataformas corporativas fornecidas por prestadores de serviços tecnológicos, incluindo *Google*, *Microsoft* e *Apple*, os quais mantêm registros de *logs* de acesso, autenticação e alterações realizadas nos dispositivos e sistemas utilizados pelos Colaboradores.

Adicionalmente, os *notebooks* utilizados pelos Colaboradores também possuem registros próprios de *logs* e eventos do sistema operacional, permitindo a rastreabilidade de acessos, autenticações, alterações relevantes e demais atividades realizadas nos equipamentos.

Tais registros permitem a auditoria dos acessos, atividades e alterações realizadas nas contas corporativas e nos equipamentos utilizados pelos Colaboradores, possibilitando a identificação de usuários, horários de acesso e eventuais desvios de utilização.

Nesse sentido, os registros e *logs* disponibilizados pelos sistemas e plataformas utilizados pela Atol Capital permitem a verificação da integridade, autenticidade e rastreabilidade dos acessos e informações, em linha com a regulamentação aplicável.

Responsabilidades do usuário

O Colaborador é responsável pelos recursos tecnológicos utilizados no exercício de suas atividades, devendo zelar pela integridade, segurança e adequado funcionamento dos equipamentos e sistemas disponibilizados pela Gestora. O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela Área de Risco, Compliance e PLD.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- a) Não compartilhar nem divulgar sua senha com terceiros;
- b) Não transportar Informações Confidenciais da Gestora em qualquer meio (CD, DVD, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;
- c) Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (transportes, restaurantes, encontros sociais, etc.);
- d) Não abrir mensagens de origem desconhecida, ou *links* suspeitos mesmo que advindos de origem conhecida;
- e) Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais, abstendo-se de utilizar redes públicas desconhecidas;
- f) Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela Atol Capital;

- g) Confirmar, por canal independente previamente cadastrado (e.g., retorno de ligação a número conhecido), qualquer instrução de pagamento, transferência, resgate ou alteração de dados bancários ou cadastrais recebida por correio eletrônico ou mensagem instantânea, ainda que aparentemente originada de pessoa conhecida; e
- h) Não inserir Informações Confidenciais ou dados pessoais em ferramentas de inteligência artificial generativa que não tenham sido previamente aprovadas pela Área de Risco, Compliance e PLD, sendo admitido apenas o uso de ferramentas corporativas cujas condições contratuais vedem a utilização dos dados inseridos para treinamento de modelos.

Proteções Adicionais aos *Notebooks*

- a) Bloqueio automático de tela em caso de inatividade, com exigência de senha para reativação do equipamento;
- b) Utilização de sistemas de antivírus nativos ou homologados, configurados para funcionamento contínuo, com realização automática de varreduras periódicas e identificação de potenciais ameaças cibernéticas;
- c) Manutenção de atualizações automáticas de segurança dos sistemas operacionais e aplicações utilizadas pelos Colaboradores, sempre que possível; e
- d) Restrições à utilização de ferramentas de acesso remoto, compartilhamento externo ou controle não autorizado dos dispositivos utilizados pelos Colaboradores.

Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Ao utilizar recursos tecnológicos da Atol Capital, o Colaborador deverá preservar a imagem da Gestora e adotar comportamento compatível com esta Política, abstendo-se de acessar conteúdos, links ou plataformas de origem suspeita ou incompatíveis com ambiente profissional.

O usuário é proibido de acessar endereços de internet (sites) que:

- a) Possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes;
- b) Possuam conteúdo ilícito, pornográfico, discriminatório ou incompatível com ambiente profissional;
- c) Não guardem relação com as atividades desempenhadas pelo Colaborador ou possam comprometer a segurança dos sistemas da Gestora;
- d) Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito baseado em sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física; e

- e) Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, ou que contenham *links* suspeitos.

Uso de correio eletrônico

É proibida a utilização de correio eletrônico particular para fins profissionais, incluindo cadastro em plataformas e sistemas, bem como para comunicação com clientes da Gestora e prestadores de serviços. É igualmente vedado o encaminhamento de Informações Confidenciais para contas de correio eletrônico pessoais, próprias ou de terceiros, sem prévia autorização da Área de Risco, Compliance e PLD.

A Atol Capital disponibiliza endereços de correio eletrônico exclusivos para cada Colaborador no desempenho de suas funções profissionais (ex.: @atolcap.com), sendo o Colaborador responsável pelo conteúdo das mensagens enviadas e pela adequada utilização de sua conta corporativa. O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Gestora, devendo ser o mesmo durante todo o seu período de vínculo com a Gestora.

A criação, alteração ou exclusão de endereço de e-mail corporativo será realizada pelo Diretor de Risco, Compliance e PLD.

Os Colaboradores estão terminantemente proibidos de criar, copiar ou encaminhar mensagens ou imagens que:

- a) Contenham declarações difamatórias, ofensivas ou incompatíveis com ambiente profissional;
- b) Façam parte de correntes de mensagens, independentemente de seu conteúdo;
- c) Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- d) Possuam conteúdo pornográfico, obsceno ou impróprio para ambiente profissional;
- e) Sejam suscetíveis de causar qualquer tipo de prejuízo a terceiros;
- f) Defendam ou possibilitem a realização de atividades ilegais;
- g) Possam prejudicar a imagem da Atol Capital; e
- h) Sejam incompatíveis com o Manual de Ética e Controles Internos da Gestora.

É proibida a reprodução, compartilhamento ou utilização de materiais recebidos por correio eletrônico ou outros meios que possam infringir direitos autorais, marcas, licenças de uso de softwares ou patentes, sem a devida autorização do titular dos respectivos direitos.

O Colaborador está ciente de que as mensagens encaminhadas por meio do correio eletrônico corporativo da Atol Capital constituem comunicações formais da Gestora, sujeitas às mesmas responsabilidades aplicáveis aos documentos corporativos tradicionais. As contas, sistemas e equipamentos utilizados no exercício das atividades da Gestora não geram expectativa de privacidade, podendo as comunicações e os arquivos corporativos ser monitorados, arquivados e acessados pela Área de Risco, Compliance e PLD, nos termos desta Política, e mantidos pelo prazo mínimo de 5 (cinco) anos.

O Colaborador, ainda, deve ser diligente em relação:

- a) Aos usuários que receberão a mensagem (Destinatário/ *To*, Copiado/*Cc* e Copiado Oculto/*Bcc*);
- b) Ao nível de confidencialidade da informação contida na mensagem;
- c) Aos anexos encaminhados, limitando o envio de arquivos ao estritamente necessário e observando o nível de confidencialidade das informações compartilhadas;
- d) Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 02 (dois) dias úteis sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

Programas de comunicação corporativa

A Atol Capital poderá contratar e utilizar aplicativos, *softwares* e ferramentas de comunicação corporativa para utilização por seus Colaboradores no exercício de suas atividades profissionais, cabendo ao Diretor de Risco, Compliance e PLD supervisionar sua utilização e verificar a adequação dos mecanismos de segurança, rastreabilidade, confidencialidade das informações e individualização dos acessos.

Os Colaboradores da Gestora também poderão utilizar aplicativos de mensagens instantâneas, incluindo WhatsApp, exclusivamente para comunicações de natureza logística (e.g., agendamentos e avisos) com Colaboradores, clientes, prestadores de serviços e contrapartes, por meio de conta vinculada a número corporativo e com solução de arquivamento que assegure a guarda das mensagens pelo prazo mínimo de 5 (cinco) anos. É vedado, contudo, o compartilhamento, encaminhamento ou circulação, por meio dessas ferramentas, de quaisquer Informações Confidenciais, bem como a transmissão ou confirmação de ordens, os quais deverão ser encaminhados exclusivamente por meio de correio eletrônico corporativo.

TREINAMENTO E CONSCIENTIZAÇÃO

A Área de Risco, Compliance e PLD promoverá treinamento em segurança da informação, segurança cibernética e proteção de dados pessoais para todos os Colaboradores, por ocasião de seu ingresso e, no mínimo, anualmente, abrangendo as ameaças descritas nesta Política, os procedimentos de reporte de incidentes, as regras de manuseio de Informações Confidenciais e a confirmação de instruções por canal independente. A participação dos Colaboradores será registrada e mantida em arquivo pelo prazo mínimo de 5 (cinco) anos.

MONITORAMENTO E TESTES PERIÓDICOS

A Área de Risco, Compliance e PLD será responsável pelo monitoramento contínuo dos controles de segurança da informação adotados pela Atol Capital, cabendo-lhe supervisionar a adequada utilização dos sistemas, plataformas, equipamentos e ferramentas tecnológicas utilizadas pela Gestora no exercício de suas atividades.

Nesse sentido, poderão ser verificados os acessos realizados aos ambientes tecnológicos da Atol Capital, os registros e logs disponibilizados pelos provedores de serviços em nuvem e pelos equipamentos utilizados pelos Colaboradores, bem como a regularidade dos mecanismos de autenticação, individualização de acessos e segregação das informações mantidas pela Gestora.

O monitoramento também compreenderá a verificação do adequado funcionamento dos mecanismos de proteção dos equipamentos utilizados pelos Colaboradores, incluindo sistemas de antivírus, atualizações de segurança e demais controles tecnológicos implementados pela Atol Capital, além da análise de eventuais incidentes, acessos indevidos, compartilhamentos não autorizados ou quaisquer eventos que possam comprometer a confidencialidade, integridade ou disponibilidade das informações da Gestora.

Dessa forma, a Atol Capital realizará, ao menos anualmente, testes e verificações relacionados aos controles internos e procedimentos previstos nesta Política, com o objetivo de avaliar sua aderência à estrutura operacional e tecnológica efetivamente adotada pela Gestora, bem como identificar eventuais necessidades de atualização, aprimoramento ou correção dos controles existentes.

As verificações realizadas poderão abranger, dentre outros aspectos, a segregação de acessos, a rastreabilidade das informações, os mecanismos de proteção dos equipamentos utilizados pelos Colaboradores e a observância das diretrizes de confidencialidade, segurança da informação e proteção de dados estabelecidas nesta Política.

Os testes anuais compreenderão, no mínimo: (i) a recertificação dos acessos concedidos; (ii) o teste de restauração de backup; (iii) a simulação de phishing com os Colaboradores; e (iv) a verificação da conformidade dos equipamentos aos requisitos da seção “Estrutura Geral de Informática”, sendo os

resultados e as medidas corretivas registrados no relatório anual de que trata o art. 25 da Resolução CVM nº 21/2021.

PLANO DE RESPOSTA

Na hipótese de identificação de incidentes relacionados à segurança da informação, acessos indevidos, vazamento de informações, indisponibilidade de sistemas ou quaisquer eventos que possam comprometer a confidencialidade, integridade ou disponibilidade das informações da Atol Capital, os Colaboradores deverão comunicar imediatamente o ocorrido ao Diretor de Risco, Compliance e PLD.

Após a identificação do evento, a Área de Risco, Compliance e PLD avaliará a natureza, extensão e potenciais impactos do incidente, podendo, conforme o caso, adotar medidas destinadas à contenção, mitigação e remediação dos riscos identificados, inclusive com o suporte de prestadores de serviços de segurança cibernética.

Os incidentes serão classificados em severidade baixa, média ou alta, considerando a natureza das informações afetadas (e.g., carteira dos fundos, dados de cotistas, dados pessoais, credenciais de acesso), sua extensão e o potencial impacto financeiro, regulatório e reputacional. Incidentes de severidade alta serão reportados imediatamente à Diretoria, a quem caberá aprovar o plano de ação, inclusive quanto à eventual comunicação a terceiros afetados ou ao mercado.

As medidas adotadas poderão incluir a restrição ou suspensão de acessos de determinados Colaboradores, redefinição de credenciais, verificação de registros e *logs*, análise dos ambientes tecnológicos afetados, recuperação de informações por meio dos mecanismos de *backup* disponíveis e demais providências técnicas e operacionais consideradas necessárias diante da natureza do incidente identificado.

A Atol Capital poderá, ainda, contratar empresa especializada de tecnologia da informação para auxiliar na identificação da origem do incidente, mensuração da extensão de eventuais vulnerabilidades, avaliação dos impactos aos sistemas e informações da Gestora, bem como para implementação de medidas corretivas, aprimoramento dos controles de segurança e recuperação dos ambientes tecnológicos afetados.

Adicionalmente, a Área de Risco, Compliance e PLD avaliará, conforme a natureza e relevância do incidente identificado, a necessidade de contratação de assessoria jurídica especializada para auxiliar na definição das medidas legais e regulatórias, incluindo eventual elaboração de plano de ação relacionado ao incidente identificado.

Sem prejuízo das demais medidas, a Área de Risco, Compliance e PLD avaliará, em até 24 (vinte e quatro) horas da ciência do incidente, a necessidade de comunicação (i) ao administrador fiduciário, ao custodiante e aos demais prestadores de serviços dos fundos e carteiras afetados; (ii) às corretoras e

plataformas cujas credenciais possam ter sido comprometidas, para bloqueio preventivo; e (iii) à ANPD e aos titulares, no caso de incidente envolvendo dados pessoais, observado o prazo previsto na seção “Obrigação de Reporte”.

A Atol Capital buscará assegurar a continuidade de suas atividades e a preservação das informações mantidas pela Gestora, observadas as diretrizes estabelecidas nesta Política e em seu Plano de Continuidade de Negócios.

Os incidentes identificados, bem como as medidas adotadas para sua contenção e tratamento, deverão ser registrados pela Área de Risco, Compliance e PLD para fins de acompanhamento, avaliação e aprimoramento dos controles internos e mecanismos de segurança da informação adotados pela Gestora, devendo tais registros ser mantidos pelo prazo mínimo de 5 (cinco) anos.

PROTEÇÃO DE DADOS PESSOAIS

Escopo e Abrangência:

A Atol Capital está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor.

Por esta razão, estabeleceu as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da Gestora, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a Gestora.

É importante observar que o escopo da proteção de dados pessoais no âmbito da Atol Capital está, em grande parte, limitado aos dados pessoais de seus Colaboradores e das pessoas naturais com as quais tiver estabelecido relações jurídicas, inclusive representantes, procuradores e beneficiários finais de pessoas jurídicas, bem como de investidores e contrapartes cujos dados sejam tratados para fins de cadastro e de prevenção à lavagem de dinheiro, nos termos da Resolução CVM nº 50/2021. Também estão abrangidos por esta proteção os dados de candidatos às vagas na Gestora, de fornecedores e outros com os quais a Gestora manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Gestora está pautado nos requisitos do artigo 7º da LGPD, assim como nas premissas do artigo 11 da mesma Lei, quando aplicável. O tratamento de dados pessoais sensíveis, por sua vez, somente poderá ocorrer nas seguintes hipóteses:

- a) Quando o titular consentir, de forma específica e destacada, para finalidades específicas;
- b) Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
 - Cumprimento de obrigação legal ou regulatória pelo controlador;
 - Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
 - Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
 - Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307/1996;
 - Proteção da vida ou da incolumidade física do titular ou de terceiros;
 - Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
 - Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Os dados pessoais não sensíveis serão tratados com fundamento nas hipóteses do art. 7º da LGPD, notadamente: (i) cumprimento de obrigação legal ou regulatória, inclusive as previstas nas Resoluções CVM nº 21/2021 e nº 50/2021; (ii) execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular; (iii) exercício regular de direitos; (iv) legítimo interesse da Gestora, observado o art. 10 da LGPD; e (v) consentimento do titular, quando nenhuma outra hipótese for aplicável.

Princípios Norteadores

A Gestora compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa-fé e nos princípios abaixo, os quais estão elencados no art. 6º da Lei 13.709/2018:

- a) Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- b) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

- c) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- d) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- e) Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- f) Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- g) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- h) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- i) Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- j) Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Direitos

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18, da Lei 13.709/2018, o titular dos dados pessoais tem direito de solicitar à Atol Capital, em relação aos seus dados, a qualquer momento e mediante requerimento expresso, o exercício dos direitos abaixo. Esses direitos estão exemplificados abaixo, todavia o seu exercício em face da Gestora deve ser analisado em cada caso concreto.

- a) Confirmação de existência de tratamento;
- b) Acesso aos dados;
- c) Correção de dados incompletos, inexatos ou desatualizados;
- d) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;

- e) Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- f) Eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na LGPD;
- g) Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- h) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
- i) Revogação do consentimento, nos termos da LGPD.

As requisições serão respondidas (i) de imediato, em formato simplificado; ou (ii) no prazo de até 15 (quinze) dias contados do requerimento, por meio de declaração clara e completa, nos termos do art. 19 da LGPD.

Responsável pela Proteção de Dados Pessoais

Em consonância com o art. 41 da Lei nº 13.709/2018, a Atol Capital salienta que o responsável por essa Política, bem como por todos os preceitos concernentes à Proteção de Dados Pessoais é o Diretor de Risco, Compliance e PLD da Gestora. O Diretor de Risco, Compliance e PLD atuará também como Encarregado pelo Tratamento de Dados Pessoais, cuja identidade e informações de contato serão divulgadas de forma clara e objetiva no site da Gestora.

A Atol Capital disponibiliza canal de comunicação específico para esse tema, através do endereço compliance@atolcap.com. O Diretor responsável pelo Tratamento de Dados Pessoais receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na LGPD em consonância com as políticas internas da Gestora.

O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como *Data Protection Officer* (DPO), é o responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade. Dessa forma, o DPO atua como uma ponte entre a Gestora, os titulares dos dados (pessoas físicas) e a Autoridade Nacional de Proteção de Dados (ANPD).

As matérias relacionadas aos dados pessoais, dados confidenciais e aos tratamentos destes poderão ser apresentadas pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação no Comitê de Risco, Compliance e PLD.

Período de Armazenamento dos Dados Pessoais

Os dados pessoais serão armazenados pela Gestora durante o período de tempo necessário para o atingimento dos objetivos para os quais foram coletados. Porém, este período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual, observado o prazo mínimo de 5 (cinco) anos previsto na Resolução CVM nº 21/2021 e na Resolução CVM nº 50/2021, após o qual os dados serão eliminados ou anonimizados, ressalvadas as hipóteses do art. 16 da LGPD.

Cooperação com Autoridades

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Gestora estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não haja vedação legal, regulatória ou judicial, inclusive o dever de sigilo previsto no art. 11, inciso II, da Lei nº 9.613/1998, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Gestora cooperará com a Autoridade Nacional de Proteção de Dados (ANPD) em qualquer problema em relação à proteção de dados e dentro dos limites previstos na LGPD e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

Transferência Internacional de Dados

Considerando que os provedores de serviços em nuvem utilizados pela Gestora podem armazenar e processar dados pessoais fora do território nacional, a transferência internacional de dados pessoais observará o art. 33 da LGPD e a Resolução CD/ANPD nº 19/2024, mediante a adoção de mecanismo válido, tais como as cláusulas-padrão contratuais aprovadas pela ANPD.

Obrigação de Reporte

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Gestora para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais comunicará à ANPD e aos titulares afetados, no prazo de 3 (três) dias úteis contados do conhecimento de que o incidente afetou dados pessoais, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos da Resolução CD/ANPD nº 15/2024.

Registro de Eventos

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos. Independentemente de comunicação à ANPD, todos os incidentes de segurança envolvendo dados pessoais serão registrados, com descrição de sua natureza, dos dados e titulares afetados, das medidas adotadas e, se for o caso, da fundamentação para a não comunicação, sendo o registro mantido pelo prazo mínimo de 5 (cinco) anos, nos termos da Resolução CD/ANPD nº 15/2024.

DISPOSIÇÕES GERAIS

Esta Política será revisada, no mínimo, a cada 12 (doze) meses, ou em prazo inferior caso haja alteração na regulamentação aplicável ou seja constatada necessidade de atualização do seu conteúdo, e suas alterações serão aprovadas pela Diretoria. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

Esta Política entra em vigor na data de sua aprovação pela Diretoria.

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE PROTEÇÃO DE DADOS, SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF sob o nº _____, declaro que li e estou plenamente de acordo com as disposições da Política de Proteção de Dados, Segurança da Informação e Cibernética da Atol Capital Gestora de Recursos Ltda. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações às quais terei acesso.

Declaro, ainda, estar ciente de que as contas, sistemas e equipamentos utilizados no exercício de minhas atividades poderão ser monitorados pela Gestora, nos termos da Política, e de que, em caso de desligamento, deverei devolver e eliminar, conforme orientação da Área de Risco, Compliance e PLD, todas as Informações Confidenciais armazenadas em equipamentos pessoais.

[Cidade], [Data]

[Assinatura]