POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO, CIBERSEGURANÇA E LGPD

AXV GESTORA DE RECURSOS LTDA.

CNPJ nº 66.292.587/0001-68

Junho/2026

ÍNDICE

1. OBJETIVO

1.1. O objetivo da presente Política de Confidencialidade, Segurança da Informação, Cibersegurança e LGPD ("Política") é estabelecer procedimentos e regras que aprimorem a segurança, tanto informacional quanto cibernética, da AXV Gestora de Recursos Ltda. ("AXV" ou "Gestora"), visando garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda. Além disso, estabelecer as medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo à consecução de suas atividades.

2. APLICAÇÃO

2.1. Esta Política aplica-se aos sócios, diretores, funcionários e demais colaboradores da AXV ("Colaboradores") que participem, de forma direta, das atividades diárias e dos negócios, representando a AXV.

3. REVISÃO E ATUALIZAÇÃO

3.1. Esta Política deverá ser revisada e atualizada anualmente, ou em prazo inferior, se assim necessário por mudanças legais, regulatórias ou autorregulatórias.

4. RESPONSABILIDADES

4.1. Os Colaboradores devem atender aos procedimentos estabelecidos nesta Política, informando quaisquer irregularidades ao Diretor de Compliance, Risco, PLD/FTP e Segurança Cibernética ("Diretor de Compliance e Risco"), que deverá avaliá-las e tomar as medidas cabíveis para garantir o atendimento a esta Política. O Diretor de Compliance e Risco é o responsável na AXV pelos temas de segurança da informação e cibernética, confidencialidade e LGPD.

5. CONTEXTO OPERACIONAL E DE NEGÓCIOS

5.1. Esta Política foi elaborada considerando as seguintes premissas e particularidades

do modelo operacional e de negócio da AXV:

(i) Todos os sistemas utilizados pela Gestora, sejam internos ou de terceiros, são acessíveis via web;

(ii) Os fornecedores dos sistemas utilizados pela AXV se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades da AXV;

(iii) Os Colaboradores estabelecem tratativas e formalizam entendimentos com clientes por meio de ferramentas e aplicativos de mensagens e/ou e-mail corporativo;

(iv) A Gestora aloca recursos mediante a utilização de plataformas acessíveis pela internet e disponíveis para qualquer dispositivo eletrônico (laptops, smartphones, tablets ou computadores de mesa);

(v) Os arquivos contendo informações pessoais e financeiras dos clientes da AXV são armazenados em nuvem, com backups automáticos;

(vi) Os dispositivos eletrônicos (laptops, smartphones, tablets) utilizados nas atividades da AXV possuem senha de acesso;

(vii) A AXV utiliza redes sem fio protegidas por senha para acesso à web de Colaboradores, prestadores de serviço ou visitantes, com redes/roteadores de redundância em caso de indisponibilidade temporária;

(viii) O escritório da AXV é o local preferencialmente utilizado para suas atividades, reuniões com clientes, comitês e reuniões comerciais, estando as rotinas e os sistemas parametrizados para serem passíveis de desempenho remoto.

6. POLÍTICA DE CONFIDENCIALIDADE

6.1. São consideradas "Informações Confidenciais" aquelas não disponíveis ao público que:

(i) identifiquem dados pessoais ou patrimoniais (da AXV ou de clientes);

(ii) sejam objeto de acordo de confidencialidade celebrado com terceiros;

(iii) identifiquem ações estratégicas dos negócios da AXV, de seus clientes ou dos portfólios sob gestão, cuja divulgação possa prejudicar a gestão ou reduzir sua vantagem competitiva;

(iv) abranjam informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, relativas às atividades da AXV, identificadas como confidenciais ou que constituam sua propriedade intelectual ou industrial, e não disponíveis ao público em geral;

(v) sejam assim consideradas em razão de determinação legal, regulamentar ou autorregulatória; e

(vi) incluam as credenciais de autenticação pessoal do Colaborador (senhas de acesso ou crachás), de uso pessoal e intransferível.

6.2. Os Colaboradores detentores de informações privilegiadas não podem compartilhar tais informações com Colaboradores que não as detenham em razão de seu cargo ou atribuição, nem com terceiros não autorizados. O acesso aos sistemas, arquivos e informações relativas às operações das carteiras é restrito aos Colaboradores que participem da área de gestão, sob supervisão do Diretor de Compliance e Risco.

6.3. Não constitui descumprimento desta Política a divulgação de Informações Confidenciais nos seguintes casos: (i) mediante prévia autorização do Diretor de Compliance e Risco; (ii) em atendimento a ordens do Poder Judiciário ou de autoridade regulatória, administrativa ou legislativa competente; e (iii) quando a divulgação se justificar, pela natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

6.4. Em caso de dúvida, o Colaborador deverá consultar previamente o Diretor de Compliance e Risco acerca da possibilidade de compartilhamento da Informação Confidencial.

7. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.1. O Colaborador que recebe ou prepara uma informação pode, se necessário, classificá-la como "Confidencial". Para tal conclusão, devem ser consideradas as questões de natureza legal e regulatória, a estratégia negocial, os riscos do compartilhamento, as necessidades de restrição de acesso e os impactos no caso de utilização indevida das informações.

7.2. Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores, mesmo quando em trabalho remoto.

7.3. Os seguintes princípios norteiam a segurança da informação na AXV:

(i) **Confidencialidade**: o acesso à informação deve ser obtido somente por pessoas autorizadas e quando de fato necessário;
(ii) **Disponibilidade**: as pessoas autorizadas devem ter acesso à informação sempre que necessário;
(iii) **Integridade**: a informação deve ser mantida em seu estado original, protegida, na guarda ou na transmissão, contra alterações indevidas, intencionais ou acidentais.

7.4. As seguintes diretrizes devem ser observadas por todos os Colaboradores:

(i) tratar as informações confidenciais de forma ética e sigilosa, de acordo com as leis e normas internas vigentes, evitando mau uso e exposição indevida;
(ii) utilizar a informação apenas para os fins para os quais foi coletada;
(iii) conceder acesso às informações confidenciais conforme o critério de menor privilégio, de modo que os usuários acessem somente os recursos imprescindíveis ao desempenho de suas atividades;
(iv) garantir identificação única, pessoal e intransferível de cada Colaborador, qualificando-o como responsável pelas ações realizadas, de forma a permitir identificar os detentores das informações para responsabilização em caso de vazamento;
(v) observar a segregação de instalações, equipamentos e informações comuns, quando aplicável;
(vi) manter a senha secreta, vedado o compartilhamento, sendo ela utilizada como assinatura eletrônica.

7.5. Qualquer risco ou falha na confidencialidade e na segurança da informação deve ser reportado ao Diretor de Compliance e Risco.

8. POLÍTICA DE CIBERSEGURANÇA

8.1. Na prestação de seus serviços, a AXV obtém e lida com informações sensíveis, não disponíveis ao público em geral. A AXV reconhece os principais riscos e ameaças aos seus ativos cibernéticos e adota medidas para preveni-los e mitigá-los. O Diretor de Compliance e Risco é o encarregado pela supervisão e mitigação dessas ameaças.

9. GESTÃO DE ACESSOS

9.1. Os serviços de rede, internet e e-mail são de propriedade exclusiva da AXV e devem ser usados com moderação para fins particulares.

9.2. A AXV poderá, mediante aprovação do Diretor de Compliance e Risco, monitorar e inspecionar o uso de e-mails, internet e aplicativos, solicitar justificativas dos usuários pelo uso de recursos e bloquear acessos ou disponibilizar recursos a terceiros, quando necessário, independentemente de prévia notificação ao Colaborador.

9.3. As senhas de acesso serão canceladas imediatamente em caso de desligamento ou transferência de área de um Colaborador.

9.4. Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à AXV.

9.5. Apenas os Colaboradores devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da AXV, mediante segregação física e lógica. Quaisquer exceções deverão ser previamente solicitadas ao Diretor de Compliance e Risco.

10. GESTÃO DE RISCOS, TRATAMENTO DE INCIDENTES, CONTINUIDADE DE NEGÓCIO E BACKUPS

10.1. Todos os riscos e incidentes de segurança devem ser reportados à área de Compliance, Risco, PLD/FTP e Segurança Cibernética, composta pelo seu Diretor e Colaboradores, que adotarão as medidas cabíveis.

10.2. O plano de contingência e de continuidade dos principais sistemas e serviços fornecidos por terceiros deve ser objeto de testes periódicos, cujos resultados o Diretor de Compliance e Risco deve solicitar e acompanhar, providenciando a solução de eventuais deficiências.

10.3. Em caso de vazamento ou acesso indevido a informação, o Diretor de Compliance e Risco deve ser comunicado imediatamente para a tomada das medidas cabíveis.

11. DIRETRIZES DE CIBERSEGURANÇA

11.1. São obrigações da AXV:

(i) Garantir a adequada proteção dos ativos cibernéticos da AXV, aí incluídos sua rede, sistemas, *softwares*, *websites*, equipamentos e arquivos eletrônicos.
(ii) Restrição e controle do acesso e privilégios de usuários não pertencentes ao quadro de Colaboradores da AXV;
(iii) Invalidar contas de Colaboradores e prestadores de serviço em seu desligamento;
(iv) Quando necessário, bloquear chaves de acesso de usuários e realizar auditoria para verificação de acessos indevidos;
(v) Excluir ou desabilitar contas inativas;
(vi) Fornecer senhas de contas privilegiadas somente a Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;
(vii) Garantir o cumprimento do procedimento de *backup* para os servidores e ativos cibernéticos, eletrônicos e computacionais da AXV;
(viii) Detectar, identificar, registrar e comunicar ao Diretor de Compliance e Risco as violações ou tentativas de acesso não autorizadas;
(ix) Organizar treinamentos relacionados à segurança dos ativos de informação sempre que necessário;
(x) Nos casos em que tais serviços e controles acima sejam terceirizados, é necessário que as condições contratuais garantam que o prestador de serviço atesta esta proteção;

(xi) Caso necessário, a partir de resultados apresentados nos testes de aderência, revisar tais práticas;

(xii) Dispor de segurança nos servidores para acesso à sua rede, visando manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados.

(xiii) Atualizar regularmente o sistema de prevenção a ataques de vírus;

(xiv) Realizar backup de arquivos de forma sistemática e os armazenar em local seguro, com monitoramento.

11.2. São obrigações dos Colaboradores:

(i) Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos; certificar-se da segurança de mensagens e anexos antes de abri-los;

(ii) Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abri-la, para evitar vírus ou códigos maliciosos;

(iii) No caso de recebimento de mensagens que contrariem as regras estabelecidas pela AXV, nunca as repassar, alertando o responsável da sua área e o Diretor de Compliance e Risco, se for o caso;

(iv) Ao se ausentar do seu local de trabalho, mesmo quando estiver trabalhando remotamente e mesmo que temporariamente, bloquear a estação de trabalho;

(v) Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail;

(vi) Utilizar equipamentos, aplicativos, impressoras, acesso a sites, e e-mail (e demais ferramentas tecnológicas) com a finalidade primordial de atender aos interesses da AXV;[1]

(vii) Tecnologias, marcas, metodologias e quaisquer informações que pertençam à AXV não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho;

(viii) Cada Colaborador terá acesso somente a pastas eletrônicas relacionadas à sua área e às pastas comuns a todos os Colaboradores.

[1] Os computadores, arquivos, e, arquivos de e-mails corporativos poderão ser inspecionados, independentemente de prévia notificação ao Colaborador, a fim de disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações.

11.3. São itens vedados aos Colaboradores:

(i) Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais[2];

(ii) Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico[3];

(iii) Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da AXV;

(iv) Alterar qualquer configuração técnica dos *softwares* que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pelo Diretor de Compliance e Risco.

11.4. Exceções a esta Política aos Colaboradores:

(i) Caso haja uso de equipamentos ou dispositivos eletrônicos de propriedade dos Colaboradores para desempenhar suas atividades na AXV, estes se comprometem a adotar as medidas de segurança anteriormente citadas a fim de preservar seus equipamentos e minimizar o risco de comprometimento de segurança às informações sensíveis da AXV, seus clientes e parceiros de negócio, podendo utilizar tais equipamentos para os diversos fins que considerar pertinentes;

(ii) É facultado ao Diretor de *Compliance* e Risco autorizar exceções a esta Política, devendo estar formalizadas por e-mail.

12. POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

12.1. A AXV, no exercício de suas atividades, coleta, armazena e realiza o tratamento de dados pessoais, conforme os parâmetros da Lei nº 13.709/2018 ("LGPD"). O tratamento ocorre nos limites estritos e nas finalidades previstas em lei e nas normas aplicáveis,

[2] Sendo proibido, sobretudo, conteúdo pornográfico, racista ou ofensivo à moral e aos princípios éticos.
[3] Exceção, é claro, a fluxos de informações necessários para a gestão de fundos e carteiras com instituições envolvidas nas operações dos clientes.

incluindo, sem limitação, as regras da CVM relativas a cadastro e identificação de clientes e operações.

12.2. O tratamento de tais dados é feito nos estritos limites e finalidades da lei e da regulação aplicável, em conformidade com a estrutura, escala e ao volume de operações da AXV, bem como à sensibilidade dos dados tratados.

12.3. Os dados pessoais, desta forma, são coletados e armazenados apenas e tão-somente para estrito cumprimento das atividades da AXV, sendo absolutamente vedada a sua destinação diversa pela AXV e/ou quaisquer de seus Colaboradores. O seu eventual uso compartilhado com reguladores e autoridades poderá ser realizado somente nos estritos termos e limites das normas vigentes aplicáveis à AXV, e para estrito cumprimento destas.

12.4. Os dados pessoais serão mantidos durante o período de vigência do relacionamento com o titular e pelo tempo exigido pelas normas legais ou regulatórias aplicáveis. Encerrado o período de tratamento, os dados serão eliminados, anonimizados ou tratados conforme previsto na LGPD.

12.5. As informações de contato da AXV a esse respeito encontram-se em seu *website*, cabendo ao Diretor de Compliance e Risco supervisionar os Colaboradores e zelar pelo tratamento de tais dados, sempre resguardados os direitos do titular contemplados no art. 18 da LGPD, quais sejam:

(i) confirmação, para o titular dos dados pessoais, da existência do tratamento destes;
(ii) acesso aos seus dados em poder da AXV;
(iii) correção de dados incompletos, inexatos ou desatualizados;
(iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
(v) 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;

(vi) eliminação dos dados pessoais tratados com o consentimento do titular (exceto, nos termos do art. 16 da LGPD, nas hipóteses de (a) cumprimento de obrigação legal ou regulatória pela AXV, (b) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD, ou (c) uso exclusivo da AXV, vedado seu acesso por terceiro, e desde que anonimizados os dados);

(vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

(viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

(ix) revogação do consentimento mediante manifestação expressa do titular.

12.6. Nas hipóteses em que o consentimento para o tratamento de dados pessoais for necessário, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, a AXV deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

13. TESTES DE ADERÊNCIA DOS CONTROLES

13.1. A efetividade desta Política é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade do Diretor de Compliance e Risco.

13.2. Os testes devem verificar se:

(i) os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;

(ii) há segregação física e lógica entre as áreas que lidem com diferentes Informações Confidenciais;

(iii) os recursos computacionais e de controle de acesso físico e lógico estão protegidos; e

(iv) a manutenção de registros permite a realização de auditorias e inspeções, bem como o cumprimento das obrigações relativas à LGPD.