

AXOR ASSET

POLÍTICA DE CONFIDENCIALIDADE, TRATAMENTO DA INFORMAÇÃO E SEGREGAÇÃO DE ATIVIDADES

Versão	Atualizada em	Responsável
1	Agosto/2026	Diretoria de Compliance, Risco e PLD

Sumário

Sumário.....	2
1. Objetivo	3
2. Base normativa.....	3
3. Abrangência	3
4. Definições.....	3
5. Governança e responsabilidades.....	4
5.1. Comitê de Risco e Compliance.....	4
5.2. Diretor responsável por controles internos e compliance.....	4
5.3. Diretor responsável pela distribuição.....	4
5.4. Colaboradores	5
6. Regras de confidencialidade e tratamento da informação	5
6.1. Princípios gerais	5
6.2. Uso e compartilhamento	5
6.3. Comunicações e registros	5
6.4. Trabalho remoto e híbrido	6
6.5. Propriedade intelectual.....	6
7. Informação privilegiada e uso indevido	6
8. Segregação de atividades	6
8.1. Diretrizes gerais	6
8.2. Segregação física	7
8.3. Segregação funcional	7
8.4. Segregação eletrônica	7
8.5. Sociedades relacionadas e prestadores compartilhados.....	7
8.6. Serviços terceirizados	8
9. Conflitos de interesses.....	8
10. Contratação de partes relacionadas	8
11. Treinamento, adesão e conscientização.....	9
12. Monitoramento e tratamento de incidentes	9
13. Violações e medidas disciplinares	9
14. Manutenção de arquivos	9
15. Vigência, aprovação e atualização	9
Anexo I - Termo de ciência e adesão	10
Histórico de Versões	11

1. Objetivo

Esta Política estabelece os princípios, as responsabilidades, as regras e os procedimentos adotados pela AXOR ASSET LTDA. ("Axor" ou "Gestora") para proteger informações, preservar sua confidencialidade, integridade, disponibilidade e uso legítimo, prevenir o uso indevido de informações privilegiadas, administrar conflitos de interesses e assegurar a adequada segregação das atividades de gestão de recursos e de distribuição de cotas dos fundos de investimento sob sua gestão.

Os controles previstos neste documento devem ser aplicados de forma proporcional à natureza, ao porte, à estrutura, ao modelo de negócio e aos riscos das atividades da Axor.

2. Base normativa

Esta Política considera, em especial, as seguintes normas, observadas suas alterações posteriores:

- Resolução CVM nº 21, de 25 de fevereiro de 2021, especialmente os arts. 22, 23, 24, 27, 28 e 34;
- Resolução CVM nº 175, de 23 de dezembro de 2022, inclusive as disposições aplicáveis ao tratamento e ao uso de informações relevantes relativas aos fundos e às classes de cotas;
- Resolução CVM nº 44, de 23 de agosto de 2021, quando aplicável ao uso, à divulgação e à negociação com informação relevante ainda não divulgada;
- Código ANBIMA de Administração e Gestão de Recursos de Terceiros e respectivas Regras e Procedimentos vigentes;
- Regras e Procedimentos de Deveres Básicos da ANBIMA, especialmente quanto a controles internos, segregação de atividades, segurança e sigilo das informações e segurança cibernética;
- Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, quando aplicável.

Em caso de conflito entre esta Política e norma legal, regulatória ou de autorregulação aplicável, prevalecerá a disposição mais específica e vigente, devendo a Política ser atualizada oportunamente.

3. Abrangência

Esta Política aplica-se aos sócios, administradores, diretores, empregados, estagiários, colaboradores, membros de comitês e prestadores de serviços da Axor que tenham acesso às suas instalações, sistemas, documentos, dados ou informações (em conjunto, "Colaboradores").

A aplicação abrange o trabalho realizado no escritório, em regime remoto ou híbrido, em viagens, reuniões externas e em qualquer ambiente no qual informações da Axor, dos fundos, das classes, dos investidores, das investidas ou de terceiros sejam acessadas ou tratadas.

4. Definições

Para fins desta Política:

- Informação Pública: informação cuja divulgação tenha sido autorizada pela Axor ou exigida por lei, regulação ou autorregulação.
- Informação Interna: informação destinada ao uso profissional interno, cuja divulgação externa não tenha sido autorizada.
- Informação Confidencial: informação não pública cujo acesso ou divulgação indevida possa causar prejuízo à Axor, aos fundos, às classes, aos investidores, às investidas, aos Colaboradores, aos prestadores de serviços ou a terceiros.
- Informação Privilegiada: informação relevante ainda não divulgada ao mercado, obtida em razão de vínculo profissional, societário, comercial ou pessoal, capaz de influenciar decisão de investimento, negociação ou exercício de direitos relacionados a valores mobiliários.
- Necessidade de Conhecimento: princípio pelo qual o acesso é concedido apenas a quem necessite da informação para cumprir atribuições profissionais legítimas.
- Barreira de Informação: conjunto de medidas físicas, funcionais, procedimentais e tecnológicas destinadas a limitar o fluxo de informações e mitigar conflitos de interesses.

5. Governança e responsabilidades

5.1. Comitê de Risco e Compliance

Compete ao Comitê de Risco e Compliance acompanhar a implementação desta Política, deliberar sobre situações relevantes, conflitos de interesses, exceções e medidas corretivas, bem como avaliar a necessidade de sua revisão.

As reuniões e deliberações relevantes do Comitê devem ser formalizadas em atas ou registros equivalentes, contendo, conforme aplicável, data, participantes, matérias analisadas, decisões, justificativas, responsáveis e prazos. Os registros devem observar acesso restrito e o prazo de guarda aplicável.

5.2. Diretor responsável por controles internos e compliance

Compete ao Diretor responsável por controles internos e compliance, com independência funcional:

- implementar, manter e supervisionar esta Política;
- orientar os Colaboradores e avaliar dúvidas, incidentes, violações e potenciais conflitos;
- aprovar, em conjunto com as áreas competentes, acessos excepcionais e medidas de segregação;
- acompanhar os serviços terceirizados que afetem confidencialidade, segregação ou segurança da informação;
- submeter ao Comitê de Risco e Compliance os assuntos relevantes; e
- assegurar a manutenção de evidências, testes, verificações e planos de ação cabíveis.

5.3. Diretor responsável pela distribuição

O Diretor responsável pela distribuição deve assegurar que a atividade se limite às cotas de fundos de investimento dos quais a Axor seja gestora, observando a regulação aplicável, as políticas internas e a separação de atribuições, acessos e responsabilidades em relação à gestão de recursos.

5.4. Colaboradores

Cada Colaborador deve conhecer e cumprir esta Política, utilizar as informações exclusivamente para fins profissionais autorizados, proteger credenciais e dispositivos, comunicar imediatamente incidentes ou suspeitas e cooperar com verificações internas. O dever de confidencialidade permanece após o término do vínculo com a Axor.

6. Regras de confidencialidade e tratamento da informação

6.1. Princípios gerais

O acesso, uso, reprodução, transmissão e armazenamento de informações devem observar finalidade profissional legítima, necessidade de conhecimento, menor privilégio, rastreabilidade e proporcionalidade. Nenhuma Informação Confidencial ou Privilegiada pode ser divulgada a pessoa que não esteja autorizada ou que não necessite conhecê-la.

Informações recebidas de investidores, administradores fiduciários, custodiante, distribuidores, investidas, consultores, assessores, prestadores ou contrapartes devem receber tratamento compatível com sua natureza, com os contratos aplicáveis e com as obrigações legais e regulatórias.

6.2. Uso e compartilhamento

É vedado ao Colaborador:

- utilizar informação da Axor ou de terceiros em benefício próprio ou alheio, fora das finalidades profissionais autorizadas;
- compartilhar documentos ou dados por e-mail pessoal, aplicativos, mídias, dispositivos ou repositórios não autorizados;
- emprestar, divulgar ou permitir o uso de suas credenciais;
- discutir informações confidenciais em locais públicos, ambientes compartilhados ou na presença de pessoas não autorizadas;
- retirar, copiar, imprimir ou descartar documentos de modo incompatível com esta Política e com a Política de Segurança da Informação e Cibernética; e
- fornecer informações à imprensa, ao público ou a terceiros em nome da Axor sem autorização.

O compartilhamento com autoridades, reguladores, autorreguladores, administradores fiduciários, auditores, assessores e prestadores será permitido quando necessário e legítimo, devendo limitar-se ao conteúdo necessário e observar meios seguros.

6.3. Comunicações e registros

As comunicações profissionais devem ser realizadas, preferencialmente, por e-mail corporativo ou por outros canais previamente autorizados. Aprovações, orientações, exceções, conflitos e decisões relevantes devem ser documentados por e-mail corporativo, ata do Comitê de Risco e Compliance ou outro registro eletrônico idôneo.

A Axor poderá monitorar, auditar e preservar comunicações realizadas por recursos corporativos, nos limites da legislação aplicável, das políticas internas e das finalidades de segurança, supervisão e cumprimento regulatório. A presente Política não pressupõe gravação de ligações telefônicas.

6.4. Trabalho remoto e híbrido

No trabalho remoto ou híbrido, os Colaboradores devem adotar cautelas adicionais, incluindo:

- utilizar equipamentos, sistemas, nuvem e canais corporativos autorizados;
- evitar redes públicas ou inseguras e impedir a visualização ou audição de informações por terceiros;
- bloquear o equipamento sempre que se ausentar e guardar documentos físicos em local seguro;
- não armazenar informações corporativas em contas, dispositivos ou repositórios pessoais; e
- comunicar imediatamente perda, furto, acesso indevido, envio equivocado ou outro incidente.

6.5. Propriedade intelectual

Documentos, bases, modelos, metodologias, relatórios, análises, apresentações, planilhas, sistemas e demais materiais produzidos ou obtidos no exercício das atividades profissionais constituem propriedade da Axor ou de terceiros que legitimamente os tenham disponibilizado. Seu uso fora das atividades autorizadas depende de aprovação prévia e do respeito aos direitos aplicáveis.

7. Informação privilegiada e uso indevido

É proibido utilizar, transmitir, recomendar ou facilitar a utilização de Informação Privilegiada para negociar valores mobiliários, cotas de fundos ou ativos relacionados, obter vantagem para si ou para terceiros, beneficiar a Axor ou influenciar decisão de investimento. Também é vedada a transmissão de recomendações, indícios ou "dicas" baseadas em Informação Privilegiada.

O Colaborador que receber, identificar ou suspeitar ter acesso a Informação Privilegiada deve:

1. interromper qualquer uso, compartilhamento ou negociação relacionada;
2. preservar o sigilo e restringir o acesso;
3. comunicar imediatamente ao Diretor responsável por controles internos e compliance; e
4. seguir as medidas determinadas, inclusive restrição de acesso, inclusão em lista de restrição, impedimento de negociação ou comunicação às autoridades, quando cabível.

A obrigação de sigilo subsiste enquanto a informação não se tornar pública por meio legítimo, sem prejuízo de obrigações que permaneçam vigentes por prazo superior.

8. Segregação de atividades

8.1. Diretrizes gerais

A Axor deve identificar, administrar e, quando necessário, eliminar conflitos capazes de afetar a imparcialidade dos profissionais envolvidos na gestão de recursos e na distribuição. A segregação será implementada por medidas físicas, funcionais, procedimentais e tecnológicas compatíveis com as atividades exercidas.

A distribuição realizada pela Axor é restrita às cotas dos fundos de investimento dos quais seja gestora. Nessa hipótese, nos termos do parágrafo único do art. 27 da Resolução CVM nº 21, não é exigida segregação física entre as áreas de gestão e de distribuição. Permanecem obrigatórias a adequada definição de atribuições, a independência das funções de controle, a proteção das informações e a administração dos conflitos de interesses.

8.2. Segregação física

A Axor mantém escritório de uso exclusivo, embora o endereço possa ser compartilhado com sociedades relacionadas. O compartilhamento de endereço não autoriza o acesso de terceiros ou de profissionais de outras sociedades às áreas, documentos, reuniões, sistemas ou informações da Axor.

O acesso às instalações e a circulação de visitantes e prestadores devem ser controlados de modo compatível com os riscos. Reuniões que envolvam Informações Confidenciais ou Privilegiadas devem ocorrer em condições que impeçam sua percepção por pessoas não autorizadas.

8.3. Segregação funcional

As responsabilidades de gestão, distribuição, risco e compliance devem observar a estrutura organizacional, as vedações de acumulação e a independência previstas na regulação. O Diretor e os profissionais responsáveis por risco e controles internos/compliance não podem atuar em funções relacionadas à gestão, intermediação, distribuição ou consultoria de valores mobiliários, nem em atividade que limite sua independência, ressalvadas as hipóteses expressamente admitidas pela regulação.

A participação de um Colaborador em comitê, fluxo de aprovação ou atividade deve respeitar sua competência e os potenciais conflitos. Quando houver conflito, o Colaborador deve informar a Diretoria de Compliance, Risco e PLD e abster-se de acessar informações ou participar da decisão até orientação formal.

8.4. Segregação eletrônica

Os arquivos da Axor são mantidos em nuvem corporativa administrada por empresa terceirizada de tecnologia da informação. A segregação eletrônica deve contemplar:

- credenciais individuais e intransferíveis;
- permissões por pasta, função e necessidade de conhecimento;
- concessão, revisão e revogação de acessos mediante processo controlado;
- proteção contra adulteração e registros que permitam auditorias e inspeções;
- backup e recuperação conforme a Política de Segurança da Informação e Cibernética e os serviços contratados;
- bloqueio tempestivo de acessos em desligamentos ou mudanças de função; e

- testes periódicos de segurança dos sistemas de informação, diretamente ou por meio do prestador especializado.

Os requisitos técnicos específicos, inclusive acesso remoto, senhas, dispositivos, incidentes, backup, continuidade e segurança cibernética, são tratados na Política de Segurança da Informação e Cibernética da Axor.

8.5. Sociedades relacionadas e prestadores compartilhados

A Axor pode compartilhar prestadores de serviços corporativos com sociedades controladoras, controladas, coligadas, sob controle comum ou relacionadas, desde que o compartilhamento não comprometa sua autonomia, a confidencialidade das informações, a independência das funções de controle, a segregação de acessos ou o tratamento dos conflitos de interesses.

O compartilhamento deve observar, conforme aplicável:

- contratação e escopo claramente definidos;
- deveres de confidencialidade e proteção de dados;
- acessos individualizados e limitados ao mínimo necessário;
- segregação lógica de pastas, ambientes, bases e credenciais;
- proibição de compartilhamento de decisões de investimento e de informações entre pessoas sem necessidade de conhecimento;
- diligência, supervisão e avaliação periódica do prestador; e
- registro e tratamento de conflitos, incidentes e exceções.

O compartilhamento de um prestador não transfere nem reduz as responsabilidades regulatórias da Axor.

8.6. Serviços terceirizados

Os serviços de tecnologia da informação e contabilidade podem ser terceirizados. A seleção, contratação e supervisão devem considerar capacidade técnica, reputação, segurança, confidencialidade, proteção de dados, continuidade, acesso às informações e possibilidade de obtenção de evidências. O acesso do terceiro deve limitar-se ao necessário para o serviço contratado e ser revogado quando deixar de ser necessário.

9. Conflitos de interesses

Conflito de interesses é a situação em que interesses da Axor, de sociedade relacionada, de Colaborador, de prestador, de fundo, de classe ou de investidor possam competir entre si ou comprometer a atuação imparcial e fiduciária.

Todo conflito real, potencial ou aparente deve ser comunicado à Diretoria de Compliance, Risco e PLD. Até a decisão, o envolvido deve abster-se de participar da análise ou deliberação e não deve acessar informações além das necessárias. As medidas possíveis incluem segregação adicional, restrição de acesso, impedimento, aprovação independente, transparência às partes, recusa ou encerramento da operação ou contratação.

Conflitos relevantes e sua solução devem ser documentados por e-mail corporativo, ata ou registro equivalente.

10. Contratação de partes relacionadas

Quando houver contratação de parte relacionada em conexão com fundo ou classe sob gestão, a Axor deve identificar previamente o vínculo e avaliar a necessidade, a capacidade técnica, a qualidade, os custos, as condições contratuais e os potenciais conflitos, observadas as competências do administrador fiduciário e as regras do regulamento.

A análise e a decisão devem ser documentadas e submetidas à Diretoria de Compliance, Risco e PLD e, quando relevante, ao Comitê de Risco e Compliance. As informações e aprovações exigidas pela regulação, pelo regulamento ou pelo administrador fiduciário devem ser providenciadas antes da contratação.

11. Treinamento, adesão e conscientização

Os Colaboradores devem receber esta Política e participar de treinamento inicial e periódico compatível com suas funções. A ciência poderá ser formalizada em termo próprio, sistema eletrônico ou e-mail corporativo que permita comprovação.

Os treinamentos devem abranger, conforme aplicável, classificação e compartilhamento de informações, trabalho remoto, conflitos, barreiras de informação, uso de credenciais, segurança cibernética, Informação Privilegiada e comunicação de incidentes.

12. Monitoramento e tratamento de incidentes

O cumprimento desta Política será monitorado pela Diretoria de Compliance, Risco e PLD, com apoio da empresa de TI e das áreas responsáveis, por meio de verificações proporcionais aos riscos, que podem incluir revisão de acessos, permissões, registros, compartilhamentos, incidentes, exceções e evidências de treinamento.

Qualquer perda, divulgação, acesso, envio, alteração ou descarte indevido, real ou suspeito, deve ser comunicado imediatamente à Diretoria de Compliance, Risco e PLD. A resposta deve contemplar contenção, preservação de evidências, avaliação de impacto, correção, plano de ação e comunicações obrigatórias, conforme a Política de Segurança da Informação e Cibernética e a legislação aplicável.

13. Violações e medidas disciplinares

O descumprimento desta Política será apurado de forma proporcional, com observância do vínculo e da legislação aplicável, podendo resultar em orientação, treinamento adicional, advertência, restrição de acesso, suspensão, desligamento, rescisão contratual, responsabilização por perdas e comunicação às autoridades competentes.

14. Manutenção de arquivos

A Axor deve manter, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior quando exigido por lei, regulação, autorregulação, contrato ou determinação de autoridade competente, os documentos, registros, correspondências, atas, evidências, relatórios, pareceres e papéis de trabalho relacionados a esta Política e ao exercício de suas funções.

Os arquivos devem ser mantidos em meio seguro, íntegro, acessível às pessoas autorizadas e apto a permitir auditorias e inspeções.

15. Vigência, aprovação e atualização

Esta Política entra em vigor na data de sua aprovação pelo Comitê de Risco e Compliance. Deve ser revisada em prazo não superior a 24 (vinte e quatro) meses e, antecipadamente, sempre que houver alteração relevante na estrutura, nas atividades, nos sistemas, nos prestadores, na legislação, na regulação ou nas regras de autorregulação, ou quando incidentes e testes indicarem necessidade de aprimoramento.

Alterações materiais devem ser aprovadas pelo Comitê de Risco e Compliance e comunicadas aos Colaboradores afetados.

Anexo I - Termo de ciência e adesão

Declaro que recebi, li e compreendi a Política de Confidencialidade, Tratamento da Informação e Segregação de Atividades da AXOR ASSET LTDA., comprometendo-me a observar integralmente suas regras, inclusive após o término do meu vínculo, quando aplicável.

Declaro também que comunicarei imediatamente à Diretoria de Compliance, Risco e PLD qualquer dúvida, conflito, incidente, violação ou suspeita relacionada a esta Política.

Nome: _____

CPF: _____

Cargo/Função: _____

Data: ____/____/____

Assinatura: _____

Histórico de Versões

As versões desta Política e as respectivas datas de aprovação encontram-se registradas abaixo.

Versão	Data	Descrição
1	Agosto/2026	Elaboração da Política