

AXOR ASSET

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

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

Sumário

1. Introdução.....	3
2. Conceitos Gerais.....	3
3. Governança e Responsabilidades.....	4
3.1. Alta Administração	4
3.2. Colaboradores e Aplicabilidade da Política.....	4
3.3. Tratamento de Exceções.....	5
3.4. Sanções	5
4. Programa de Segurança da Informação e Cibernética.....	5
4.1. Princípios de Segurança da Informação	5
4.2. Identificação e Avaliação de Riscos.....	5
4.3. Classificação da Informação	5
4.4. Ações de Prevenção e Proteção	6
4.4.1. Controle de Acesso e Senhas.....	6
4.4.2. Estações de Trabalho e Dispositivos	6
4.4.3. Uso de Correio Eletrônico e Internet	6
4.4.4. Uso de Dispositivos Pessoais.....	6
4.4.5. Acesso Remoto e Trabalho a Distância	7
4.4.6. Criptografia	7
4.4.7. Prevenção a Vazamento de Dados.....	7
4.5. Armazenamento e Computação em Nuvem.....	7
4.6. Controle, Monitoramento e Testes.....	7
4.7. Plano de Resposta a Incidentes.....	7
5. Contratação e Monitoramento de Terceiros	8
6. Confidencialidade das Informações	8
7. Treinamento e Capacitação	8
8. Vigência e Atualização	8
9. Manutenção dos Arquivos.....	9
Anexo I. Termo de Ciência e Adesão	10
Anexo II. Matriz de Avaliação de Riscos.....	11
Histórico de Versões	12

1. Introdução

A presente **Política de Segurança da Informação e Segurança Cibernética** (“Política”) da **AXOR ASSET** (“Gestora”) estabelece as diretrizes, princípios e regras adotados pela Gestora para assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a auditabilidade das informações e dos sistemas utilizados no exercício de suas atividades, bem como para prevenir, detectar e responder a incidentes de segurança cibernética.

Esta Política foi elaborada em observância à **Resolução CVM nº 21, de 25 de fevereiro de 2021**, conforme alterada (“RCVM 21”), ao **Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros** (“Código ART”) e ao **Guia ANBIMA de Cibersegurança**, em sua 4ª edição (2025), cujas recomendações orientam a estrutura do programa de segurança da Gestora.

O tratamento de dados pessoais pela Gestora, nos termos da **Lei nº 13.709, de 14 de agosto de 2018** (“LGPD”), é disciplinado em documento próprio, a **Política de Proteção de Dados Pessoais** da Gestora, que complementa esta Política no que se refere à segurança aplicada aos dados pessoais. As duas políticas são de observância conjunta.

A proteção das informações e dos ativos tecnológicos da Gestora é dever de todos os sócios, administradores, funcionários e estagiários (“Colaboradores”), bem como dos prestadores de serviços e terceiros que, em razão de suas funções, acessem informações ou o ambiente tecnológico da Gestora.

2. Conceitos Gerais

Segurança da Informação: conjunto de regras, controles e práticas destinado a preservar a confidencialidade, a integridade e a disponibilidade das informações, independentemente da forma ou do meio em que se apresentem, sejam escritas, faladas, digitais ou impressas.

Segurança Cibernética: conjunto de medidas voltadas à proteção dos sistemas, redes, dispositivos e dados contra ameaças e ataques originados no ambiente digital, bem como à detecção e à resposta a tais eventos.

Ativos de Informação: dados, sistemas, equipamentos, aplicativos, redes e demais recursos utilizados pela Gestora para processar, armazenar ou transmitir informações.

Incidente de Segurança: qualquer evento, confirmado ou sob suspeita fundamentada, que comprometa ou possa comprometer a confidencialidade, a integridade ou a disponibilidade das informações ou dos sistemas da Gestora, incluindo acessos não autorizados, vazamentos, indisponibilidades e ataques cibernéticos.

Informações Confidenciais: informações críticas para os negócios da Gestora ou de seus clientes cuja divulgação não autorizada possa causar impactos financeiros, reputacionais, operacionais ou sujeitar a Gestora a sanções.

Ameaças Cibernéticas: métodos empregados para comprometer sistemas e informações, tais como programas maliciosos (vírus, cavalo de troia, spyware e ransomware), engenharia social (phishing,

vishing, smishing e phishing), ataques de negação de serviço (DDoS), invasões persistentes avançadas e ameaças potencializadas por inteligência artificial, tais como fraudes por deepfake de voz ou vídeo e mensagens de phishing geradas por inteligência artificial.

3. Governança e Responsabilidades

A estrutura, o cumprimento e os assuntos relacionados à segurança da informação e à segurança cibernética da Gestora são de responsabilidade do diretor estatutário responsável pela implementação e cumprimento de regras, procedimentos e controles internos, nos termos da RCVIM 21 ("Diretor de Compliance, Risco e PLD"), a quem compete implementar e manter esta Política.

A Gestora administra internamente seu ambiente de tecnologia da informação, podendo contratar de terceiros de reconhecida reputação serviços e ferramentas especializados (tais como computação em nuvem, correio eletrônico e soluções de segurança), sempre sob supervisão da Diretoria de Compliance, Risco e PLD. As atribuições técnicas de tecnologia da informação da Gestora são exercidas por essa estrutura interna ("TI").

Compete à Diretoria de Compliance, Risco e PLD, sem prejuízo de outras atribuições previstas nesta Política:

- (a) implementar, divulgar e manter atualizada esta Política, observados a natureza, o porte e o perfil de risco da Gestora;
- (b) coordenar a identificação e a avaliação periódica dos riscos de segurança da informação e cibernética;
- (c) supervisionar a implementação dos controles de prevenção, proteção, monitoramento e resposta previstos nesta Política;
- (d) conduzir o plano de resposta a incidentes e classificar sua severidade;
- (e) promover treinamentos periódicos e a cultura de segurança entre os Colaboradores;
- (f) avaliar a segurança de prestadores de serviços relevantes e de serviços em nuvem, na forma desta Política; e
- (g) registrar e arquivar os incidentes e as medidas adotadas, reportando-os à Alta Administração.

3.1. Alta Administração

A Alta Administração da Gestora, composta por seus diretores estatutários nomeados em contrato social ("Alta Administração"), tem as seguintes responsabilidades:

- (a) aprovar esta Política e suas atualizações;
- (b) estar tempestivamente ciente dos principais riscos de segurança da informação e cibernética a que a Gestora está exposta;
- (c) assegurar que o Diretor de Compliance, Risco e PLD tenha independência, autonomia e recursos suficientes para o cumprimento desta Política; e
- (d) assegurar a alocação de recursos humanos, tecnológicos e financeiros adequados ao programa de segurança.

3.2. Colaboradores e Aplicabilidade da Política

Esta Política aplica-se a todos os Colaboradores e, no que couber, aos prestadores de serviços e terceiros que acessem informações ou o ambiente tecnológico da Gestora, sendo parte integrante das regras que regem a relação societária, de trabalho ou contratual, conforme o caso. Todos os Colaboradores devem zelar por seu cumprimento e reportar imediatamente à Diretoria de Compliance, Risco e PLD qualquer incidente ou suspeita de incidente de segurança.

3.3. Tratamento de Exceções

Circunstâncias específicas, controles mitigantes já existentes ou motivo legítimo demonstrável podem justificar solicitação de exceção às regras desta Política. Eventuais exceções devem ser amplamente documentadas e justificadas e dependem de avaliação e manifestação do Diretor de Compliance, Risco e PLD, com validação final pela Alta Administração.

3.4. Sanções

O descumprimento, a suspeita ou o indício de descumprimento de quaisquer das normas desta Política deverá ser levado à apreciação do Diretor de Compliance, Risco e PLD, que poderá aplicar as medidas disciplinares cabíveis aos Colaboradores, na forma do Código de Ética e Conduta da Gestora, sem prejuízo das consequências legais aplicáveis.

4. Programa de Segurança da Informação e Cibernética

O programa de segurança da Gestora observa os cinco pilares recomendados pelo Guia ANBIMA de Cibersegurança: (i) identificação e avaliação de riscos; (ii) ações de prevenção e proteção; (iii) controle, monitoramento e testes; (iv) plano de resposta a incidentes; e (v) governança, esta última disciplinada na Seção 3 acima.

4.1. Princípios de Segurança da Informação

Toda informação coletada, gerada ou processada por Colaboradores ou terceiros no exercício das atividades da Gestora constitui ativo da Gestora e deve ser utilizada exclusivamente para finalidade legítima e relacionada às suas atividades. Independentemente da forma ou do meio, as informações devem ser protegidas de acordo com sua criticidade, observados os princípios da confidencialidade, integridade, disponibilidade, autenticidade e auditabilidade.

4.2. Identificação e Avaliação de Riscos

A Gestora identifica e avalia periodicamente os processos, ativos, sistemas e dados relevantes ao seu funcionamento, mapeando vulnerabilidades, ameaças e cenários de risco, de modo a dimensionar seus impactos financeiro, reputacional e operacional e a definir as ações de prevenção e proteção adequadas. A avaliação dos riscos, o respectivo risco residual após os controles e as ações de mitigação estão consolidados na matriz do Anexo II desta Política, revista sempre que houver alteração relevante no ambiente tecnológico ou no perfil de risco da Gestora.

4.3. Classificação da Informação

As informações são classificadas segundo sua criticidade, de modo a receber proteção proporcional quanto ao acesso e ao uso:

Pública: informação destinada ou passível de divulgação ao público em geral, de caráter informativo, comercial ou promocional, ou cuja publicidade decorra de exigência legal.

Interna: informação de circulação restrita aos Colaboradores e terceiros contratados, cujo acesso indevido por terceiros deve ser evitado.

Confidencial: informação crítica para os negócios da Gestora ou de seus clientes, restrita a grupo específico de pessoas, cuja divulgação não autorizada possa causar impactos relevantes ou sanções.

Restrita: informação acessível apenas a pessoas expressamente indicadas, cuja divulgação não autorizada possa comprometer seriamente a estratégia ou os negócios da Gestora, tais como posições, estratégias de investimento e demais informações relacionadas à gestão das carteiras.

Informações internas, confidenciais e restritas não devem ser tratadas em locais públicos ou na presença de pessoas não autorizadas. A comunicação de qualquer informação da Gestora à imprensa, ao público ou a órgãos externos depende de autorização prévia da Diretoria de Compliance, Risco e PLD.

4.4. Ações de Prevenção e Proteção

A Gestora adota controles proporcionais à criticidade de seus ativos e informações, revisados periodicamente pela TI sob supervisão da Diretoria de Compliance, Risco e PLD.

4.4.1. Controle de Acesso e Senhas

- Os acessos são concedidos segundo o princípio do menor privilégio, limitados ao estritamente necessário ao desempenho das funções de cada Colaborador.
- A criação, alteração e exclusão de usuários e permissões são realizadas pela TI mediante autorização da Diretoria de Compliance, Risco e PLD.
- A autenticação é individual e intransferível, exigindo-se senhas de complexidade adequada e a utilização de **múltiplo fator de autenticação (MFA)** nos sistemas e serviços que o suportem.
- A concessão, a alteração e a revogação de acessos acompanham a movimentação do Colaborador, procedendo-se à revogação tempestiva de credenciais e acessos no desligamento (offboarding).
- Eventos de autenticação e alteração de credenciais são auditáveis e rastreáveis.

4.4.2. Estações de Trabalho e Dispositivos

- Os equipamentos disponibilizados destinam-se exclusivamente ao desempenho das atividades profissionais e possuem sistema operacional, antivírus e demais proteções atualizados.
- A instalação de softwares e a alteração de configurações dependem de autorização prévia, sendo permitido apenas o uso de programas homologados pela Gestora.
- Os equipamentos corporativos, em especial os portáteis (notebooks), adotam criptografia de disco, de modo a proteger as informações em caso de perda ou furto.
- As estações de trabalho possuem bloqueio automático por inatividade e a conexão de dispositivos móveis de armazenamento depende de autorização prévia.
- As informações são objeto de rotinas periódicas de cópia de segurança (backup).

4.4.3. Uso de Correio Eletrônico e Internet

- O correio eletrônico corporativo é individual, intransferível e de propriedade da Gestora, disponibilizado no domínio corporativo da Gestora e destinado ao uso profissional. É vedado o uso profissional de correio eletrônico particular, salvo contingência autorizada.
- É vedado abrir mensagens ou links de origem desconhecida ou suspeita e reproduzir conteúdo que infrinja direitos de terceiros ou seja incompatível com o Código de Ética e Conduta da Gestora.
- O Colaborador é responsável pelos acessos e comunicações realizados com sua autenticação, devendo resguardar a imagem da Gestora e evitar o acesso a sítios de origem não segura.

4.4.4. Uso de Dispositivos Pessoais

O uso de dispositivos pessoais para fins profissionais, quando admitido, observa as orientações da Gestora quanto à segurança (bring your own device), exigindo-se controles de acesso e proteção compatíveis com os aplicáveis aos equipamentos corporativos e sujeitando-se à autorização prévia da Diretoria de Compliance, Risco e PLD. A Gestora pode adotar solução de gerenciamento de dispositivos móveis (MDM) para impor controles mínimos de segurança e, quando necessário, remover remotamente os dados corporativos do dispositivo.

4.4.5. Acesso Remoto e Trabalho a Distância

O acesso remoto aos sistemas e às informações da Gestora ocorre por meio de conexão segura, com uso de rede privada virtual (VPN) corporativa e autenticação individual, observados os mesmos controles aplicáveis ao ambiente interno. A Gestora pode adotar controles adicionais de verificação contínua de confiança no acesso, segundo o modelo de confiança zero (zero trust).

4.4.6. Criptografia

As informações confidenciais e restritas são protegidas por criptografia, tanto em repouso quanto em trânsito, de acordo com sua criticidade, adotando-se protocolos e algoritmos de mercado e a gestão adequada das chaves criptográficas, de modo a preservar a confidencialidade e a integridade das informações.

4.4.7. Prevenção a Vazamento de Dados

A Gestora adota medidas para prevenir a exfiltração e o vazamento de informações, incluindo, na medida de sua estrutura, controles de prevenção à perda de dados (DLP), o princípio do menor privilégio, a revogação tempestiva de acessos no desligamento e a manutenção de termos de confidencialidade, sem prejuízo do disposto na Seção 6.

4.5. Armazenamento e Computação em Nuvem

A Gestora poderá armazenar informações e utilizar serviços de computação em nuvem de fornecedores de reconhecida reputação técnica, prezando pela confidencialidade, integridade, disponibilidade e recuperabilidade das informações. A contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, observa as regras da Seção 5 desta Política.

4.6. Controle, Monitoramento e Testes

A Gestora mantém monitoramento contínuo de seu ambiente tecnológico e inventário atualizado de ativos relevantes. Os registros (logs) de sistemas e de acessos são mantidos e verificados de modo a preservar a integridade, a autenticidade e a auditabilidade das informações e sistemas, nos termos da RCVM 21.

Em observância ao art. 24, II, da RCVM 21, a Gestora assegura a realização de testes periódicos de segurança dos sistemas de informação. Entre esses testes, a Gestora realiza, periodicamente, testes de intrusão (pentest) e varreduras de vulnerabilidade, com a adoção tempestiva das correções pertinentes, podendo contar com o apoio de empresa especializada independente. Os testes de contingência são realizados na periodicidade e na forma previstas no Plano de Continuidade de Negócios da Gestora, ao qual esta Política se integra.

4.7. Plano de Resposta a Incidentes

Identificado ou havendo suspeita fundamentada de incidente de segurança, inclusive decorrente de ataque cibernético, serão adotadas, de forma tempestiva, as medidas de contenção, investigação, erradicação e recuperação cabíveis, coordenadas pela Diretoria de Compliance, Risco e PLD com o apoio da TI, incluindo, conforme o caso:

- (a) verificação e auditoria dos registros (logs) e identificação das informações potencialmente afetadas;
- (b) isolamento dos sistemas afetados, eliminação de agentes maliciosos e restauração de dados a partir das cópias de segurança;
- (c) avaliação das consequências reputacionais, operacionais e jurídicas do incidente; e
- (d) comunicação aos clientes e às autoridades afetadas, quando cabível.

Sempre que o incidente envolver dados pessoais, o tratamento do evento, a avaliação de risco aos titulares e a eventual comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares observarão o disposto na Política de Proteção de Dados Pessoais da Gestora.

Todo incidente e as respectivas medidas serão classificados por nível de severidade, documentados e arquivados pela Diretoria de Compliance, Risco e PLD e, quando aplicável, registrados no Relatório de Controles Internos da Gestora. Poderá ser contratada empresa especializada para apoio na resposta ao evento.

5. Contratação e Monitoramento de Terceiros

Prestadores de serviços e terceiros podem representar fonte relevante de risco cibernético. A contratação de serviços de processamento e armazenamento de dados e de computação em nuvem observa avaliação prévia da capacidade e da confiabilidade do fornecedor, verificando-se, no mínimo:

- (i) o acesso da Gestora aos dados e informações processados ou armazenados pelo prestador;
- (ii) a confidencialidade, a integridade, a disponibilidade e a recuperabilidade das informações;
- (iii) a aderência do prestador a certificações exigidas pela Gestora ou por reguladores, quando aplicável;

- (iv) o provimento de informações e recursos adequados ao monitoramento dos serviços; e
- (v) a segregação e a proteção dos dados por meio de controles físicos ou lógicos adequados.

Para essa avaliação, a Gestora poderá utilizar o Questionário ANBIMA de Due Diligence para Contratação de Terceiros e Serviços em Nuvem (QDD), disponibilizado pela ANBIMA, observado, ainda, o disposto na Política de Seleção, Contratação e Monitoramento de Terceiros da Gestora.

6. Confidencialidade das Informações

Nenhuma Informação Confidencial poderá ser divulgada a terceiros não autorizados. Os Colaboradores comprometem-se a utilizar as informações a que têm acesso estrita e exclusivamente para o desempenho de suas atividades na Gestora, mantendo sigilo durante e após o vínculo, na forma do Termo de Ciência e Adesão (Anexo I) e das demais políticas da Gestora. Os prestadores de serviços cujos contratos contenham cláusula de confidencialidade estão dispensados de assinatura de termo específico.

7. Treinamento e Capacitação

A Gestora promove treinamentos periódicos sobre segurança da informação e cibernética, abrangendo prevenção, identificação e resposta a incidentes e boas práticas de uso dos recursos tecnológicos, com o objetivo de disseminar a cultura de segurança entre os Colaboradores.

8. Vigência e Atualização

Esta Política será revisada em até 24 (vinte e quatro) meses, ou sempre que o Diretor de Compliance, Risco e PLD e/ou a Alta Administração entender necessário, sem aviso prévio. As alterações serão divulgadas a todos os sócios, diretores e Colaboradores pela Diretoria de Compliance, Risco e PLD e ficarão disponíveis para consulta no repositório de políticas de compliance da Gestora.

9. Manutenção dos Arquivos

A Gestora manterá armazenados eletronicamente todos os arquivos pertinentes ao processo de compliance desta Política por período mínimo de 5 (cinco) anos, ou por prazo superior em caso de determinação da CVM ou de processo administrativo em curso, conforme a legislação vigente.

ANEXO I

TERMO DE CIÊNCIA E ADESÃO

Declaro que li e compreendi integralmente a Política de Segurança da Informação e Segurança Cibernética da AXOR ASSET, com a qual estou plenamente de acordo, comprometendo-me a observar suas disposições e a preservar a confidencialidade das informações às quais tiver acesso, durante e após o meu vínculo com a Gestora.

Nome: _____

CPF: _____

São Paulo, _____ de _____ de 20____.

Assinatura

ANEXO II

MATRIZ DE AVALIAÇÃO DE RISCOS

Para cada processo ou ativo relevante, a Diretoria de Compliance, Risco e PLD avalia as ameaças, a classificação da informação, o grau de exposição e o impacto inerentes, o risco residual após a aplicação dos controles, o responsável pelo monitoramento e as ações de prevenção e proteção, conforme mapeamento abaixo, revisto periodicamente.

Processo / Ativo	Ameaça	Classificação	Grau de Exposição	Impacto	Risco Residual	Responsável	Ações de Prevenção e Proteção
Sistemas e dados em nuvem	Malware / Ransomware	Confidencial / Restrita	Alto	Alto	Médio	Compliance / TI	Antivírus e sistemas atualizados; backups periódicos; provedores de nuvem de boa reputação; controle de acesso por perfil; logs e trilha de auditoria.
Sistemas e dados em nuvem	Ataques de DDoS	Confidencial	Baixo	Médio	Baixo	Compliance / TI	Provedores de nuvem com proteção contra indisponibilidade; monitoramento; plano de continuidade.
Servidor de arquivos / documentos	Invasões	Confidencial / Restrita	Médio	Alto	Médio	Compliance / TI	Firewall e antivírus atualizados; controle de acesso centralizado conforme inventário; logs e trilha de auditoria.
Documentos físicos com dados de terceiros	Engenharia social	Confidencial	Médio	Médio	Baixo	Compliance	Política de mesa limpa; armazenamento seguro; descarte seguro de documentos.
Correio eletrônico e comunicação	Phishing / invasão de e-mails	Interna / Confidencial	Médio	Médio	Baixo	Compliance / TI	Provedores de e-mail de boa reputação; MFA; filtros anti-spam; treinamento de Colaboradores.
Contratação de serviços em nuvem (país e exterior)	Ameaças diversas ao prestador	Confidencial	Alto	Alto	Médio	Compliance	Due diligence prévia com o Questionário ANBIMA (QDD); verificação de acesso, confidencialidade, integridade, disponibilidade e recuperabilidade dos dados.
Endpoints e trabalho remoto (notebooks e acesso remoto)	Comprometimento de dispositivo ou acesso remoto inseguro	Interna / Confidencial	Médio	Médio	Baixo	Compliance / TI	Criptografia de disco; VPN corporativa; MDM; antivírus e atualização; bloqueio por inatividade.
Informações e credenciais internas	Ameaça interna / vazamento (insider)	Confidencial / Restrita	Médio	Alto	Médio	Compliance / TI	Menor privilégio; revogação de acessos no desligamento; DLP; termos de confidencialidade (NDA); trilhas de auditoria.
Sistemas e aplicações	Exploração de vulnerabilidades	Confidencial	Médio	Alto	Médio	Compliance / TI	Gestão contínua de vulnerabilidades; testes de intrusão (pentest) e varreduras periódicas; aplicação tempestiva de correções.
Dados em repouso e em trânsito	Interceptação ou acesso indevido a dados	Confidencial / Restrita	Médio	Alto	Baixo	Compliance / TI	Criptografia em repouso e em trânsito; gestão de chaves; protocolos seguros de comunicação.



Os graus de exposição, impacto e risco residual acima são revisados periodicamente pela Diretoria de Compliance, Risco e PLD, à luz do ambiente tecnológico e dos controles efetivamente implementados pela Gestora.

Histórico de Versões

As versões desta Política e as respectivas datas de aprovação encontram-se registradas abaixo. O detalhamento das alterações de cada revisão é mantido nos registros internos de aprovação da Alta Administração.

Versão	Data	Descrição
1	Agosto/2026	Elaboração da Política.
2	Agosto/2026	Inclusão de controles de endpoints, acesso remoto (VPN), criptografia, prevenção a vazamento (DLP) e testes de vulnerabilidade; matriz de riscos com risco residual, responsável e classificação.