# POLÍTICA DE SEGURANÇA CIBERNÉTICA

**AVVERO ASSET GESTÃO DE RECURSOS LTDA.**

| Área Responsável: | Acesso: | Data Versão: |
|---|---|---|
| Compliance e Risco | Público | 10/10/2025 |

**SUMÁRIO**

# 1. INTRODUÇÃO E OBJETIVO

A Política de Segurança Cibernética ("Política") estabelece os princípios, conceitos, valores e práticas a serem adotados visando assegurar a confidencialidade, a integridade e a disponibilidade das informações de posse temporária, de propriedade da AVVERO ASSET GESTÃO DE RECURSOS LTDA. ("AVVERO ASSET" ou "Gestora"), permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade.

A segurança da informação está entre um dos tópicos mais relevantes dentro de uma organização. As informações fazem parte do patrimônio da empresa e estão sob constante risco. A sua perda ou roubo representa um prejuízo significativo para a estratégia do negócio. Dessa forma, a confidencialidade, integridade e disponibilidade da informação são pilares diretamente ligados ao tema de Segurança.

Com o objetivo de minimizar esses riscos, a Política tem como finalidade estabelecer princípios e diretrizes de proteção de dados pessoais e informações sigilosas contra ameaças cibernéticas.

# 2. ABRANGÊNCIA E DEFINIÇÕES

Todos os sócios, funcionários, menores aprendizes, estagiários e prestadores de serviços ("Colaboradores") e partes interessadas da AVVERO ASSET que tenham acesso concedido às informações de posse temporária ou de propriedade da Gestora, em qualquer meio (físico e/ou eletrônico), ou aos sistemas e recursos computacionais estão sujeitos a essa Política, exceto quando houver contrato estabelecido com cláusulas de proteção e sigilo.

A responsabilidade em relação à segurança da informação deve ser comunicada aos Colaboradores no início do vínculo com a Gestora, devendo estes assinarem o Acordo de Confidencialidade, de forma manual ou eletrônica, quando permitido por lei.

# 3. PROTEÇÃO DA BASE DE DADOS

Os recursos computacionais da Gestora devem ser: (i) protegidos contra adulterações; e (ii) permitir a realização de auditorias e inspeções.

Todos os registros eletrônicos realizados pela Gestora deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que a Gestora tenha atuação.

As informações mantidas em meios eletrônicos devem ser salvas em bases replicadas (backups) e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso deverá ser limitado somente a pessoas autorizadas pela área de Compliance.

No âmbito de infraestrutura e ambiente, são adotados (as):

- Manutenção Preventiva.
- Sistemas Críticos com Redundância;
- Contingenciamento de Energia;
- Sistemas de Backup;
- Segurança Física; e
- Atualizações Automáticas.

## 4. POLÍTICA PARA DISPOSITIVOS PESSOAIS

Os Colaboradores deverão comunicar à área de Compliance sua opção por utilizar seus dispositivos pessoais, como smartphones e laptops, para acesso à rede corporativa, sistemas internos e bancos de dados.

Os dispositivos devem ser constantemente monitorados pela AVVERO ASSET para resguardar possíveis violações à política de segurança e incidentes.

A área de Compliance poderá auditará o dispositivo, e poderá instalar ferramentas de monitoramento e remoção remota de informações (para caso de roubo ou perda do dispositivo) e somente aprovará seu uso se o Colaborador concordar em:

- Acompanhar treinamentos de segurança promovidos periodicamente pela área de Compliance;
- Aprovar a gestão de soluções móveis da AVVERO ASSET, que contém, dentre seus principais termos, os seguintes pontos:
    - Ações para bloqueamento remoto,
    - Remoção completa de arquivos,
    - Restauração aos padrões de fábrica; e
    - Monitoramento constante de atividades realizadas no dispositivo.
- Seguir os procedimentos definidos nesta Política em casos de incidentes como roubo ou extravio do dispositivo pessoal;

- Utilizar sempre a versão mais atualizada do sistema operacional e efetuar todas as atualizações do fabricante;
- Utilizar autenticação de múltiplos fatores (2FA) em todos os sistemas da AVVERO ASSET;
- Não utilizar logins pessoais para qualquer tarefa relacionada à AVVERO ASSET;
- Não emprestar o dispositivo para terceiros, inclusive membros da família;
- Evitar links ou anexos de e-mails de fontes não confiáveis; e
- Retornar o dispositivo à área de Compliance, no caso de desligamento, para sanitização.

## 5. DAS SANÇÕES

O não cumprimento das normas estabelecidas nessa Política, seja isolada ou cumulativamente, poderá acarretar, de acordo com a infração cometida, as seguintes sanções:

- Comunicação informando o descumprimento ao Compliance e reporte ao Comitê de Compliance.
- Advertência ou Suspensão para casos graves ou na hipótese de reincidência de infrações de menor gravidade.
- Desligamento para casos graves ou reincidência de advertências/suspensões.

## 6. SEGURANÇA CIBERNÉTICA

Este capítulo da Política tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética da AVVERO ASSET. Assim, deverá ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

As diretrizes aqui abordadas seguem práticas de mercado, bem como está de acordo com as leis, regulamentação e autorregulação aplicáveis, incluindo o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros e o Guia de Cibersegurança.

O objetivo das regras sobre segurança cibernética da AVVERO ASSET é, primordialmente, assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir

que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da AVVERO ASSET devem assegurar:

- a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário); e
- a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da AVVERO ASSET, observadas as regras de sigilo e confidencialidade constantes do Capítulo de segurança da informação.

A AVVERO ASSET exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

## 7. RESPONSÁVEL PELA SEGURANÇA CIBERNÉTICA

O Diretor de Compliance é o principal responsável dentro da AVVERO ASSET para tratar e responder questões de segurança cibernética (“Responsável pela Segurança Cibernética”), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

Segue abaixo uma lista, não exaustiva, dos deveres e responsabilidades do Responsável pela Segurança Cibernética:

- Testar a eficácia dos controles utilizados e informar ao Comitê de Segurança Cibernética os riscos residuais.
- Acordar com o Comitê de Segurança Cibernética os serviços prestados por terceiros contratados e os procedimentos de resposta aos incidentes.
- Acompanhar a configuração dos equipamentos e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos.

- Avaliar os controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da AVVERO ASSET em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da AVVERO ASSET, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da AVVERO ASSET.
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da AVVERO ASSET, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente, deverá imediatamente informar o Responsável por Segurança Cibernética, que poderá convocar reunião do Comitê de Segurança Cibernética.

## 8. COMITÊ DE SEGURANÇA CIBERNÉTICA

O Comitê de Segurança Cibernética será composto pelo: (i) Diretor de Compliance, (ii) sócios majoritários da AVVERO ASSET e (iii) membros da equipe de tecnologia e infraestrutura, tendo como objetivo a supervisão e monitoramento das regras de segurança cibernética, conforme aqui previsto.

O Comitê de Segurança Cibernética se reunirá de forma extraordinária, sempre que necessário, mediante convocação e deverá ser instalado necessariamente com a presença do Responsável pela Segurança Cibernética, a quem caberá a sua coordenação. As decisões deverão ser lavradas em ata das reuniões e registradas pela área de Compliance.

## 9. DEMAIS ATRIBUIÇÕES

Caberá a todos os Colaboradores conhecer e adotar as disposições desta Política, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas, o qual recorrerá ao Responsável pela Segurança Cibernética, se for o caso.

Em caso de incidente que afete a segurança cibernética da AVVERO ASSET, o Colaborador deverá comunicar imediatamente seu superior ou Diretor de Compliance. Em caso de descumprimento, ainda que involuntário, estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei.

## 10. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Todos os requisitos de segurança da informação e segurança cibernética, incluindo a necessidade de planos de contingência, devem ser previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e documentados e testados durante a fase de execução.

Periodicamente, no mínimo anualmente, a AVVERO ASSET deverá revisar o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas de forma.

## 11. AÇÕES DE PREVENÇÃO E PROTEÇÃO

A AVVERO ASSET estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles. Cada Colaborador tem responsabilidade em manter o controle e segurança das informações armazenadas ou disponibilizadas em seus equipamentos.

### 11.1. Internet, e-mail e computadores

A AVVERO ASSET oferece a seus Colaboradores uma completa estrutura tecnológica para o exercício de suas atividades. É de responsabilidade do Colaborador manter e zelar pela integridade dessas ferramentas de trabalho.

Além disso, o Colaborador é responsável pela proteção de seu banco de dados, seja ele composto por planilhas, e-mails e/ou conversas telefônicas contendo dados confidenciais de clientes e/ou da AVVERO ASSET, dentre outros.

- Os equipamentos e computadores utilizados pelos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da AVVERO ASSET e sob nenhuma hipótese servirão de instrumento à qualquer forma não autorizada expressamente em lei;
- A utilização de equipamentos da AVVERO ASSET para fins particulares é permitida de forma moderada;
- Os downloads de qualquer natureza devem ser feitos de forma ponderada e com a devida diligência por parte do usuário, respeitando o espaço individual de cada usuário.
- Periodicamente e sem aviso prévio serão realizadas inspeções nos computadores para averiguação de downloads impróprios não autorizados ou gravados em local indevido;
- O correio eletrônico disponibilizado pela AVVERO ASSET caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas. É permitida a utilização pessoal de forma moderada;
- As mensagens enviadas ou recebidas através do correio eletrônico corporativo (os "e-mails corporativos"), seus respectivos anexos, e a navegação através da rede mundial de computadores (a "Internet") através de equipamentos da AVVERO ASSET serão monitoradas; e
- Os E-mails Corporativos recebidos pelos Colaboradores, quando abertos, deverão ter sua adequação às regras desta Política imediatamente verificada. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem.

11.2. Senhas

As senhas fornecidas aos Colaboradores para acesso à rede corporativa e sistemas internos, são de caráter sigiloso, pessoal e intransferível, sendo os Colaboradores os responsáveis pela manutenção de cada senha e suas características.

11.3. Monitoramento Telefônico

As conversas telefônicas originadas ou recebidas pelo sistema de telefonia da AVVERO ASSET poderão ser monitoradas e gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política, inclusive no âmbito judicial.

11.4. Monitoramento por câmeras

A AVVERO ASSET pode utilizar serviço de monitoramento por câmeras e são gravadas de modo que o conteúdo possa ser usado para fins de esclarecimento de questões relacionadas a esta Política.

## 12. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA DE TERCEIROS

Os Colaboradores externos da AVVERO ASSET, dentre os quais os seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de cibersegurança. Esses riscos devem ser levados em conta pela AVVERO ASSET.

12.1. Avaliação dos Terceiros Contratados

A contratação de terceiros se pautará, no que tange à segurança cibernética e conforme se verificará em diligência específica, pelos seguintes critérios:

- Possuir políticas, programa e procedimentos formais relativos à segurança da informação que sejam auditados e atualizados periodicamente.
- Política formalizada de segurança cibernética, e atualização de suas certificações necessárias à prestação dos serviços contratados.
- Disponibilização de plano de resposta a incidentes de segurança cibernética.
- Realização de ações de conscientização, educação e formação de segurança de seus funcionários.
- Possuir, comprovadamente, mecanismos satisfatórios para proteção dos dados transacionados com a AVVERO ASSET.
- Canal de Compliance adequado para o reporte completo e tempestivo de incidentes de segurança cibernética.

Nesse sentido, a área de Compliance deverá realizar diligência para o tema de segurança cibernética de terceiros que (i) gerem acesso a informações e sistemas confidenciais ou sensíveis, (ii) prestem serviços de computação em nuvem, (iii) tenham conexões lógicas (links) com a AVVERO ASSET ou (iv) qualquer outros que a área de Compliance julgue que

por qualquer motivo possa gerar risco de cibersegurança à AVVERO ASSET, previamente à sua contratação, na forma do Anexo I a esta Política.

O resultado da diligência será avaliado em Comitê de Segurança Cibernética, devendo a decisão ser formalizada e periodicamente reavaliada.

12.2. Requisitos de Segurança da Informação nos Contratos com Terceiros

A AVVERO ASSET deverá incluir em contratos com Colaboradores externos requisitos de segurança da informação nos contratos de prestação de serviços, bem como verificar a efetividade dos controles implementados pela empresa contratada para atender aos requisitos durante a vigência do contrato, na forma menciona acima.

## 13. GOVERNANÇA

A AVVERO ASSET deverá manter o programa de segurança cibernética continuamente atualizado, com o objetivo de identificar tanto novos riscos como reavaliando riscos residuais.

Também realizará, periodicamente, campanha de conscientização em cibersegurança com o fim de garantir que todos os Colaboradores tenham as informações necessárias para atuar no tema.

O Responsável pela Segurança Cibernética, em conjunto com o Comitê de Segurança Cibernética, realizará a revisão e atualização desta Política periodicamente, no mínimo anualmente ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança Cibernética.

# ANEXO I - MODELO DE DILIGÊNCIA COM TERCEIROS DO GRUPO TÉCNICO DE CIBERSEGURANÇA DA ANBIMA

Conteúdo mínimo de Compliance em segurança cibernética a ser verificado

| Compliance | **Respostas** |
|---|---|
| 1. A empresa tem políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança? a. Se sim, é objeto de teste ou auditoria periódica? b. Se não, está em fase de elaboração? Qual é o prazo de finalização dele para devido envio à instituição contratante? | |
| 2. A empresa apresenta plano de resposta a incidentes de cibersegurança? | |
| 3. A empresa apresenta ações de conscientização, educação e formação de segurança da informação junto a seus funcionários? | |
| 4. Quais são as ferramentas e os mecanismos utilizados para proteção de dados transacionados com a empresa contratante? | |
| 5. Quais são as práticas aplicadas para detectar atividade não autorizadas nos sistemas utilizados? Solicitar também designação de responsável por detectar tais atividades e a quem se reporta. | |
| 6. Na eventualidade de detecção de incidente de cibersegurança, o relato é feito por meio de canais de gestão apropriadas o mais rápido possível? Há comunicação a clients e/ou reguladores (quando aplicável)? | |
| Favor disponibilizar os seguintes documentos:<br><br>Programa de segurança cibernética: se a organização segue políticas, programa e procedimentos formais relativos a segurança da informação e cibersegurança, recomenda-se solicitar envio da documentação à empresa contratante para avaliação e arquivamento. Solicitar também o último relatório de teste/auditoria periódica.<br><br>Certificações: solicitar envio de certificações que possam comprovar a devida capacidade técnica do prestador de serviço. | |