POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

AVVERO ASSET GESTÃO DE RECURSOS LTDA.

Área Responsável:	Acesso:	Data Versão:
Compliance e Risco	Público	01/10/2025

SUMÁRIO

1. INTRODUÇÃO E OBJETIVO

A Política de Segurança da Informação ("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. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

A Avvero Asset adota as seguintes diretrizes de segurança da informação, que visam garantir um nível adequado de proteção ao seu ambiente de negócios:

- As informações da Avvero Asset, dos clientes e público em geral devem ser tratadas de forma ética e sigilosa, de acordo com as leis vigentes e normas internas.
- As informações devem ser utilizadas de forma transparente e apenas para as finalidades alinhadas.

- Os procedimentos e os controles deverão abranger todo o processo de autenticação, prevenção e detecção de intrusão, com a realização de testes periódicos.
- O acesso dos usuários às informações e ambiente da Avvero Asset deverá ser controlado.
- Somente deve ser concedido acesso aos recursos imprescindíveis para o pleno desempenho das atividades do usuário autorizado.
- A senha é utilizada como assinatura eletrônica, sendo pessoal e intransferível. Ela deve ser mantida de forma secreta, sendo proibido o seu compartilhamento.
- Devem ser reportados eventuais fatos ou ocorrências que possam colocar a Gestora em risco.
- As responsabilidades se aplicam a todos os Colaboradores, que deverão declarar entendimento e ciência conforme programa de Compliance.

4. CONTROLES DE ACESSO A INFORMAÇÕES CONFIDENCIAIS

Para fins desta Política, entende-se como Informação Confidencial toda informação resguardada contra a revelação pública não autorizada, ou seja, informações eletrônicas, escritas ou faladas da qual o Colaborador tiver acesso dentro da Gestora, incluindo: dados da Avvero Asset, seus sócios, diretores, colaboradores, clientes e fornecedores, bem como de relatórios de órgãos reguladores, autorreguladores e do poder público, dados de inspeções e fiscalizações, materiais de marketing e demais informações de propriedade da Gestora.

4.1. Acesso a sistemas de informações digitais

Todo acesso a diretórios e sistemas de Informações Confidenciais da Avvero Asset deve ser controlado. Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores previamente autorizados pela área de Compliance. O controle do acesso a sistemas de informações da Avvero Asset levará em conta as seguintes premissas:

- Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil e área de atuação;
- Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora; e
- Manutenção de documentos digitais por prazo não inferior a 5 (cinco) anos.
- As senhas deverão possuir no mínimo 8 caracteres alfanuméricos, incluindo letras maiúsculas e minúsculas.

- Os diretores são responsáveis pela concessão de acessos aos colaboradores de sua área, bem como a manutenção e revisão a cada 12 meses.

Ainda, como medidas de prevenção:

- Comunicação – divulgação sobre ocorrências e formatos recentes de fraudes e incidentes;
- Habilitação de relatos de ameaças pelos usuários – fornecimento de canal seguro para análise de ameaças recebidas;
- Validação – realização de testes periódicos para avaliação da prontidão dos colaboradores e equipe de suporte interno; e
- Revisão – revisão dos acessos aos sistemas de informação a cada 12 meses.

4.2. Acesso às instalações físicas

A gestora prioriza o armazenamento de informações sempre em via digital, em que os colaboradores tenham acesso mediante definições do item 4.1. No que se refere às instalações físicas, cada colaborador terá acesso às instalações mediante chave ou cadastro de senha numérica pessoal e intransferível ou biometria.

5. BARREIRAS E CONTROLE DE INFORMAÇÕES

Os Colaboradores detentores de Informações Confidenciais ou informações não públicas relevantes ("Informações Privilegiadas"), em função de seus cargos ou atribuições na Gestora, devem estabelecer uma barreira de informações para os demais Colaboradores. De forma não exaustiva, as seguintes condutas devem ser observadas:

- Os Colaboradores devem evitar circular em ambientes externos à Avvero Asset com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, salvo se necessárias ao desenvolvimento do projeto e no interesse do cliente, devendo essas cópias ser criptografadas ou mantidas através de senha de acesso;
- As informações que possibilitem a identificação de um cliente da Gestora devem se limitar a arquivos de acesso restrito e apenas poderão ser copiadas ou impressas se forem para o atendimento dos interesses da Avvero Asset ou do próprio cliente;
- Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos;
- O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, com orientação da equipe de segurança e infraestrutura;

- A senha de acesso do Colaborador ao sistema da Avvero Asset é pessoal e intransferível, conforme já destacado nas diretrizes acima;
- Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes etc.;
- O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora, e poderá ser monitorado pela área de Compliance sempre que necessário.

6. DETENTORES DA INFORMAÇÃO, MANUTENÇÃO DE REGISTROS E LOGS

O Diretor de Compliance deve manter o registro dos Colaboradores que detenham Informações Privilegiadas, com a indicação do tipo de informação detida, e devendo informar aos Sócios os casos que possam significar restrição nas operações da Avvero Asset.

Será atribuído a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que os usuários (login) individuais de Colaboradores internos serão de responsabilidade do próprio e os usuários (login) de terceiros serão de responsabilidade do diretor da área contratante. Assim, é possível realizar a identificação dos detentores da informação.

Estas medidas foram desenvolvidas para evitar situações que possam suscitar um provável conflito de interesses ou a má utilização de informações. Desta forma, minimizando prováveis ameaças aos negócios e à imagem da Avvero Asset.

Com relação ao monitoramento e auditoria do ambiente, a Gestora possui sistemas de monitoramento nos servidores e correio eletrônico. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado. O monitoramento dos controles de segurança adotará a abordagem baseada em risco, intensificado, assim, de acordo com o nível de risco.

A Gestora informa, ainda, que poderá tomar as seguintes medidas:

- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação da Diretora de Compliance;
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade; ou
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;

- Gravação de ligações telefônicas realizadas e recebidas por ramais;
- Com a ciência de todos os participantes, reuniões presenciais na sede da gestora e reuniões realizadas por meio digital em plataformas como Zoom, Teams, Meet, entre outras, serão gravadas; e
- As gravações serão mantidas pelo prazo de 5 anos.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas da Gestora e sujeitará o usuário às sanções administrativas e legais cabíveis, observado o disposto no Item 11 desta Política.

7. CONSIDERAÇÕES SOBRE DADOS PESSOAIS

Em atendimento à Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais ("LGPD"), destaca-se que toda informação relacionada a pessoa natural identificada ou identificável ("Dados Pessoais") e dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, vinculados a uma pessoa natural ("Dados Pessoais Sensíveis") eventualmente coletados pela Avvero Asset têm finalidades específicas e pré-determinadas para seu tratamento, sendo certo que todos os critérios e diretrizes de confidencialidade e sigilo previstos nesta Política se estendem a eles.

Ainda, a Avvero Asset adota os melhores esforços técnicos e administrativos para garantir que todos os processos de armazenamento, compartilhamento, acesso e eliminação dos Dados Pessoais e Dados Pessoais Sensíveis por ela tratados estejam adequados à LGPD e melhores práticas do mercado.

8. TESTES E TREINAMENTOS DE SEGURANÇA DA INFORMAÇÃO

Como forma de garantir a implementação de ambiente adequado, a Avvero Asset se reserva o direito de:

- Implantar softwares e sistemas que podem monitorar e gravar os acessos e uso de Internet através da rede e das estações de trabalho da empresa, respeitado o direito à intimidade e ao sigilo das comunicações, nos termos do art. 5º, X e XII, da Constituição Federal;
- Inspecionar qualquer arquivo, estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta Política;
- Efetuar verificações e/ou auditoria coordenada por área interna ou contratada em sistemas, estações e rede sem aviso prévio.

A área de Tecnologia e Segurança é responsável pela implementação dos testes periódicos e ações preventivas para detectar falhas de segurança e vulnerabilidades, inclusive na adoção de novas tecnologias. Além disso, anualmente, serão realizados testes de invasão e varreduras para detectar vulnerabilidades em sistema, softwares e infraestrutura da Gestora. No caso de detecção de falha ou uso em desconformidade com o estabelecido na Política, serão aplicados bloqueios de acesso e/ou planos de ação corretivos.

A apresentação sobre o programa de segurança da informação fará parte do treinamento inicial e periódico da Gestora, e deverá assegurar que todos os Colaboradores tenham conhecimento dos procedimentos e das obrigações previstas nesta Política, assim como minimizar a ocorrência de incidentes de segurança.

9. TRATAMENTOS DE INCIDENTES

Em caso de suspeita ou incidente de violação das normas de segurança da informação identificado pelo Colaborador, a área de Tecnologia e Segurança deverá ser notificada imediatamente com o objetivo de realizar análise e levantamento dos sistemas e informações afetadas. Ademais, a documentação completa do incidente deverá ser registrada e enviada para avaliação do Compliance.

Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da Avvero Asset.

Os incidentes de segurança da informação identificados ou relacionados com a Avvero Asset possuem caráter sigiloso.

10. 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.

11. 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.

12. 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.