POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ASA INVESTMENTS

Termo	Definição
ANBIMA	Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais.
Colaborador	Todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, de estágio, comercial, profissional, contratual ou de confiança com as sociedades da Gestora
CVM	Comissão de Valores Mobiliários
Diretor de Compliance	É o diretor estatutário da Gestora indicado em seu Formulário de Referência como responsável pelo cumprimento de regras, políticas, procedimentos e controles internos e pelo combate e prevenção à lavagem de dinheiro e ao financiamento do terrorismo.
Gestora	Asa Asset 2 Gestão de Recursos Ltda (“Asa Investments” ou “Gestora”)
Guia ANBIMA de Cibersegurança	É o Guia de Cibersegurança editado pela ANBIMA em dezembro de 2017.
Gestor de Segurança da Informação	Colaborador responsável pelos temas relacionados à segurança da informação.

Objetivo

O objetivo desta política é orientar e direcionar todos os colaboradores da Gestora com acesso aos dados e sistemas corporativos a manusear as informações de maneira segura, protegendo assim os dados de acesso não autorizado e ameaças externas (Virus, Worm, Engenharia Social, Ciberataques, entre outros).

Segurança da Informação e Cibernética

As medidas de segurança da informação têm por finalidade mitigar as ameaças que podem comprometer a boa reputação da Gestora.

Assim, a presente Política de Segurança da Informação e Segurança Cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gestora.

A coordenação direta das atividades relacionadas à Política de Segurança da Informação e Segurança Cibernética ficará a cargo do Gestor de Segurança da Informação, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos colaboradores, conforme aqui descrito.

Identificação de Riscos (Risk Assessment)

No âmbito de suas atividades, a Gestora identificou os principais aspectos e componentes que precisam de proteção:

- Dados e Informações: as informações confidenciais, incluindo informações a respeito de investidores, clientes, colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- Sistemas: informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio e compliance da Gestora;
- Governança da Gestão de Risco: a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, foram identificadas as seguintes ameaças, em linha com o disposto no Guia de Cibersegurança da ANBIMA:

- Malware softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware e Ransomware);

- Engenharia Social: métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);
- Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- Invasões (advanced persistent threats): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base nas ameaças relacionadas acima, o time de Segurança da Informação da Gestora e a Diretoria de Compliance devem avaliar e definir o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

Ações de Prevenção e Proteção

- Regras Gerais

A Gestora realiza o efetivo controle do acesso a arquivos que contemplem informações confidenciais em meio físico, disponibilizando-os somente aos colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise.

As informações geradas internamente, adquiridas no mercado ou absorvidas pela Gestora são consideradas patrimônio, devendo ser tratadas como ativo e confidencial. No caso de exceção, informações cuja divulgação seja obrigatória ao mercado e clientes por exigência de órgãos reguladores devem ser cuidadosamente avaliadas e aprovadas pela Diretoria de Compliance. Tal autorização deve ser respeitada durante todo o ciclo de vida desta informação.

Todos os recursos da informação, sejam eles tecnológicos ou não, devem ser utilizados exclusivamente para o desenvolvimento de atividades profissionais referentes aos negócios da Gestora.

- Uso da Internet

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à Gestora.

O acesso à internet é de responsabilidade de cada usuário, ficando vedado o acesso a sites com conteúdo impróprio, ilegal ou que possam comprometer a segurança dos dados e o bom funcionamento dos sistemas.

Com o objetivo de mitigar o vazamento de informações corporativas, webmails ou qualquer site pessoal que seja possível o upload de dados deve ser bloqueado.

- Uso de e-mail

É vedado o uso de e-mails externos não pertencentes à Gestora. O uso do correio eletrônico para envio e recepção de mensagens deverá ocorrer apenas através dos sistemas oficiais da empresa. Os colaboradores devem evitar a utilização do e-mail corporativo para assuntos pessoais.

Como o objetivo de proteger as informações da companhia, não é permitido o envio de qualquer conteúdo corporativo para o e-mail pessoal do colaborador.

- Apps Corporativos no Celular ou Outros Dispositivos

Algumas medidas devem ser consideradas ao usar o celular/demais dispositivos:

1. Em caso de roubo, furto ou perda do aparelho, o time de TI da Gestora deve ser notificado imediatamente para iniciar a exclusão remota dos dados corporativos.
2. As informações corporativas disponíveis no aparelho não devem ser compartilhadas com terceiros/familiares.
3. Em caso de desligamento do colaborador, o time de TI deverá remover remotamente os dados corporativos.

- E-mails Indesejáveis

E-mail de remetentes desconhecidos / indesejáveis devem ser manipulados com cuidado, conforme orientação abaixo:

1. Anexos ou links neste tipo de e-mail não devem ser abertos/clicados devido ao risco de infecção por vírus ou ciberataque.
2. Não responder o e-mail, pois a resposta confirmará a validade do endereço de e-mail do colaborador. Tal confirmação poderá ser utilizada para o envio de futuros spams.
3. E-mails suspeitos devem ser reportados para o Time de TI

- Uso de Mídia removível

A mídia removível é um ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais, nesse caso, os modens 5G e pen drive merecem especial atenção. Portanto, uso de tais mídias sem o conhecimento do time de TI não é permitido. Exceções quanto ao uso deste tipo de mídia nos computadores deve ser aprovado pelo Time de Compliance e tratada como exceção à regra.

.

- Mesa Limpa

Para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente, os papéis com informações corporativas e mídia eletrônica devem ser armazenados em armários trancados adequados e/ou em outras formas de mobiliário de segurança, quando não estiverem em uso, especialmente fora do horário do expediente.

- Bloqueio do Computador

Para evitar a exposição das informações ou o acesso não autorizado ao computador, todas as vezes que o colaborador se ausentar da sua estação de trabalho o bloqueio da tela deve ser feito manualmente, digitando um conjunto de botões do teclado (Ctrl+Alt+Del).

- Senha e Login

A senha e login para acesso à rede interna, ou qualquer sistema corporativo, devem ser conhecidos pelo respectivo usuário e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. A senha deverá conter no mínimo 8 caracteres alfanuméricos e ser alterada pelos colaboradores a cada 45 dias.

O colaborador pode ser responsabilizado, inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

- Uso de Equipamentos e Sistemas

Cada colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

Todo colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas, deve comunicar seu superior hierárquico ou a Diretoria de Compliance.

Softwares e hardwares não devem ser instalados nos computadores sem o conhecimento do Time de TI.

- Acesso Escalonado ao Sistema

O acesso como “administrador” à rede interna deve ser limitado aos usuários, com isso, serão *determinados níveis de acesso* de usuários apropriados para os colaboradores.

Os níveis de acesso a pastas, arquivos eletrônicos e sistemas devem estar alinhado com o perfil de acordo com as funções e responsabilidades do colaborador.

- Destruição de Documentos

O descarte de documentos corporativos deve ser feito em picotadoras. Tal tipo de conteúdo não deve ser descartado em um lixo comum, pois eles podem ser facilmente recuperados, assim expondo a informação que deveria estar protegida.

- Falar em Público

Atenção ao falar sobre a empresa, clientes ou negócios em lugares públicos (táxis, elevadores, transporte público, restaurantes, cafés, etc.) pois informações corporativas podem ser expostas, afetando negativamente a reputação da companhia.

Portanto, é de extrema importância ter cuidado ao falar publicamente sobre informações confidenciais e internas.

- Acesso Remoto

A Gestora permite o acesso remoto pelos colaboradores, com os mesmos acessos verificados no escritório, entretanto a conexão com a internet deverá ser feita a partir de local seguro, tais como a residência ou conexão pelo celular. Devido ao risco de invasão por hackers, o uso de wifi público (aeroporto, cafés, restaurante, lojas, etc.) não deve ser utilizado para o acesso remoto.

Ademais, os colaboradores autorizados devem ser instruídos a (i) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (ii) relatar ao time de Segurança da Informação a violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Gestora e que ocorram durante o trabalho remoto, e (iii) não armazenar informações corporativas em dispositivos pessoais.

Quando o acesso remoto for utilizado, todas as orientações informadas nesta política devem ser aplicadas.

- Sistema em Nuvem

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos da Gestora e serviço de armazenamento de dados em nuvem, em conta dedicada, que não poderão ser compartilhados com outras empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

- Software, Varreduras e Backup

O Time de TI deve manter atualizados os sistemas de proteção contra malware e virus nos seus dispositivos.

Com o objetivo de detectar e eliminar ameaças cibernéticas tais como malware e vírus, o Time de TI deve manter os sistemas de proteção atualizados e executar varreduras periódicas nos computadores.

A Gestora também deverá manter e testar regularmente medidas de backup consideradas apropriadas pelo Gestor de Segurança da Informação. As informações da Gestora são atualmente objeto de back-up diário com o uso de computação na nuvem.

- Conscientização e Treinamento

Com objetivo de orientar os colaboradores sobre como identificar e reagir as diferentes ameaças relacionadas à proteção das informações, e as quais atualmente estamos expostos, todos os colaboradores devem participar do treinamento de segurança da informação que deve ser oferecido periodicamente em linha com as disposições da Política de Treinamento e Certificação da Gestora. Tal treinamento também deve compor o kit onboarding.

Monitoramento e Teste de Controle

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos fornecidos pela Gestora se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos colaboradores, a Gestora poderá monitorar o conteúdo trafegado em tais sistemas, tais como:

- Navegação na internet;
- Envio e recebimento de e-mail;
- Acesso a arquivos na rede;
- Sistemas corporativos providos pela companhia.

A da Diretoria de Compliance, no exercício regular de suas funções, poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de violação, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer informações corporativas, mesmo que de forma involuntária, deverá ser informada ao Time de Segurança da Informação. Com base na criticidade do incidente, o Time de Segurança da Informação deverá reportar prontamente o evento à Diretoria de Compliance, que será responsável pela avaliação do caso.
Ademais, a Diretoria de Compliance determinará quais terceiros, se houver, deverão ser contatados com relação à violação.

- Incidente envolvendo dados pessoais

Sem prejuízo do quanto exposto nesta seção, os incidentes de segurança envolvendo Dados Pessoais deverão ser geridos e tratados de acordo com o documento Plano de Resposta a Incidentes envolvendo Dados Pessoais da Gestora.

- Avaliação do Incidente

Primeiramente será via Time de Segurança da Informação, que será o responsável pela avalição técnica, de acordo com os critérios abaixo:

1. Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

2. Identificação dos sistemas afetados, se houver, devem ser desconectados ou de outra forma desabilitados;

3. Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

Após a avaliação técnica, a Diretoria de Compliance será responsável pela:

1. Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, administrador fiduciário, clientes ou investidores afetados, segurança pública);

2. Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da informação, se privilegiada);

3. Determinação do responsável que arcará com as perdas decorrentes do incidente, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

- Procedimentos de Resposta

Após a avaliação técnica do incidente, as ações abaixo devem ser executadas pelo time de Segurança da Informação:

Contenção: ações imediatas para interromper o desenvolvimento do incidente no menor intervalo de tempo possível.

Erradicação: medida para sanar o problema de forma definitiva.

Recuperação: identificar o último estado bom conhecido do serviço, restaurar de backups para esse estado.

Caso a Diretoria de Compliance julgue necessário, as ações abaixo devem ser executadas:

1. Notificação às partes internas e externas apropriadas (por exemplo, administrador fiduciário, clientes ou investidores afetados, segurança pública);

2. Publicação do fato ao mercado, nos termos da regulamentação vigente.

3. Notificação do responsável que arcará com as perdas decorrentes do incidente.

Arquivamento de Informações

Os colaboradores deverão manter arquivada toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria interna e/ou externa ou investigação de órgãos regulatórios em torno de possíveis atuações da Gestora, investimentos e/ou situações em que haja suspeita de corrupção e/ou da prática de crimes de lavagem de dinheiro e financiamento ao terrorismo, conforme o caso em conformidade com o inciso IV do Artigo 16 da Instrução CVM 558.

Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Gestora, tais como minutas de contrato, memorandos, cartas, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Gestora, razão pela qual o colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, sendo vedado ao colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Gestora.

Revisão da Política

O Gestor de Segurança da Informação deverá realizar a revisão desta política anualmente, no mínimo, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais, devendo submeter sua revisão/avaliação à Diretoria de Compliance, que poderá incluir no relatório anual de *Compliance* as eventuais deficiências encontradas.

A finalidade de tal revisão será assegurar que os procedimentos aqui previstos permaneçam consistentes com as operações comerciais da Gestora e acontecimentos regulatórios relevantes.

HISTÓRICO DAS ATUALIZAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Histórico das atualizações desta Política		
Data	**Versão**	**Responsável**
Janeiro de 2020	1ª	Diretora de Compliance
Dezembro de 2020	2ª	Diretora de Compliance
Maio de 2021	3ª	Diretora de Compliance
Junho de 2021	4ª	Diretora de Compliance e Risco
Outubro de 2021	5ª	Diretora de Compliance
Junho de 2022	6ª	Gestor de Segurança da Informação

Histórico das aprovações desta Política		
Data	**Versão**	**Responsável**
Junho de 2022	6ª	Diretor de Compliance