POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

FAMILY OFFICE

Definições

Termo	Definição
ANBIMA	Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais.
Código ANBIMA de ART	Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.
Colaborador	Todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, de estágio, comercial, profissional, contratual ou de confiança com as sociedades do ASA
CVM	Comissão de Valores Mobiliários
Departamento de Seleção	É a área interna do ASA Family Office responsável pela seleção e contratação de novos profissionais.
Diretora de Compliance	É o diretor estatutário do ASA Family Office indicado em seus respectivos Formulários 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.
Diretor de Distribuição	Quando aplicável, é o diretor estatutário indicado como responsável pela atividade de distribuição das respectivas sociedades que integram o do ASA Family Office.
Diretor de Investimentos	É o respectivo diretor estatutário responsável pela administração de carteiras de valores mobiliários do ASA Family Office, conforme identificado em seus respectivos Formulários de Referência.
Gestora	É a Asa Asset Gestão em Investimentos Ltda. (“Asa Family Office“).
Guia ANBIMA de Cibersegurança	É o Guia de Cibersegurança editado pela ANBIMA em Dezembro de 2017.
Recursos Humanos	É a Equipe de Recursos Humanos do do ASA Family Office.

Segurança da Informação e Cibernética

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios do ASA.

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 pelo ASA.

A coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Diretoria de Compliance, 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, o ASA identificou os seguintes principais aspectos e componentes que precisam de proteção:

- Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da 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 do ASA;
- Governança da Gestão de Risco: a eficácia da gestão de risco pelo ASA 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 principais 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 no acima, o Asa Family Office avalia e define 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

O Asa Family Office 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 pelo Asa Family Office 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 deve ser cuidadosamente avaliada e aprovada pela da 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 do Asa Family Office.

- 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 ao Asa Family Office.

O acesso às páginas e web sites é de responsabilidade de cada usuário, ficando vedado o acesso a sites com conteúdo impróprio.

- Uso de Mídia removíveis

O uso de mídias removíveis no Asa Family Office não é estimulado, devendo ser tratado como exceção à regra.
A mídias removíveis é o principal 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.

- Uso de e-mail

É vedado o uso de sistemas e-mail externos, não pertencentes ao Asa Family Office. O uso do correio eletrônico para envio e recepção de e-mail deverá ocorrer apenas através sistema oficial da empresa. Os colaboradores devem evitar a utilização de o e-mail da empresa para assuntos pessoais.

Deve-se assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio.

Não deve-se executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

- Acesso Escalonado ao Sistema

O acesso como “administrador” à rede interna será limitado aos usuários, com isso, serão determinados níveis de acesso de usuários apropriados para os Colaboradores.

O ASA, mantêm diferentes níveis de acesso a pastas e arquivos eletrônicos, notadamente aqueles que contemplem Informações Confidenciais, de acordo com as funções e responsabilidades dos Colaboradores e pode monitorar o acesso dos Colaboradores a tais pastas e arquivos com base na senha e login disponibilizados.

- Senha e Login

A senha e login para acesso à rede interna, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas a cada 60 dias, conforme aviso fornecido pelo responsável pela área de tecnologia

Dessa forma, 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.

- Acesso Remoto

O Asa Family Office permite o acesso remoto pelos Colaboradores, com os mesmos acessos verificados no escritório.

Ademais, os Colaboradores autorizados serão instruídos a (i) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (ii) relatar ao Comitê de Compliance violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações do Asa Family Office e que ocorram durante o trabalho remoto, e (iii) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos do Asa Family Office e serviço de armazenamento de dados em nuvem (OneDrive, Microsoft), em conta dedicada, que não poderão ser compartilhados com outras empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, o Asa Family Office monitora a utilização de tais meios.

- Software, Varreduras e Backup

O Asa Family Office manterá proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, vírus, worms, spyware).

Serão conduzidas varreduras periodicamente para detectar e eliminar qualquer ameaça em termos de cibersegurança.

O Asa Family Office também manterão e testarão regularmente medidas de backup consideradas apropriadas pela da Diretoria de Compliance. As informações do ASA Family Office são atualmente objeto de back-up diário com o uso de computação na nuvem.

Monitoramento e Testes

Em linha com o disposto acima, o Asa Family Office:

(a) mantem diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e cargos dos Colaboradores e pode monitorar o acesso dos Colaboradores a tais pastas e arquivos com base na senha e login disponibilizados;

(b) pode monitorar o acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos; e

Ainda, 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.

O treinamento dos Colaboradores com relação às regras e procedimentos acima serão organizados periodicamente, em linha com as disposições da Política de Treinamento e Certificação do Asa Family Office.

Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de violação, acesso não autorizado, outro comprometimento da rede ou dos dispositivos do Asa Family Office (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada a Segurança da informação e com base da criticidade do incidente, será reportado e avaliado pelo Comitê de Compliance prontamente.

Ademais, a Diretoria de Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação.

- Procedimentos de Resposta

Primeiramente será via Segurança da informação e com base da criticidade do incidente, será reportado e avaliado pelo Comitê de Compliance, onde será respondido qualquer informação de suspeita de violação, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos do Asa Family Office de acordo com os critérios abaixo:

(i) 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;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

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

(vi) 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);

(vii) Determinação do responsável que arcará com as perdas decorrentes do incidente, após a condução de investigação e uma avaliação completa das circunstâncias 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 do Asa Family Office, 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 ao Asa Family Office 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 do Asa Family Office, 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 do Asa Family Office, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento do Asa Family Office.

Revisão da Política

A Diretoria de Compliance deverá realizar uma revisão desta Política de Segurança da Informação e Cibernética a cada 12 (doze) meses, no mínimo, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos

residuais, incluindo no relatório anual de *Compliance* eventuais deficiências encontradas.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais do Asa Family Office 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
Novembro de 2021	6ª e Atual	Diretora de Compliance