POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

AGOSTO/2020

SUMÁRIO

1. Apresentação

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") se aplica às administradoras de carteiras de títulos e valores mobiliários, na modalidade gestora de recursos, nos termos da Instrução CVM nº 558, de 26 de março de 2015, conforme alterada ("ICVM 558"), do Grupo Navi, quais sejam, Navi Capital - Administradora e Gestora de Recursos Financeiros Ltda. ("Navi Capital"), Navi Yield – Administradora e Gestora de Recursos Financeiros Ltda. ("Navi Yield"), Navi Allocation - Administradora e Gestora de Recursos Financeiros Ltda. ("Navi Allocation"), Navi Real Estate Selection - Administradora e Gestora de Recursos Financeiros Ltda. ("Navi Selection"), Navi Real Estate Ventures - Administradora e Gestora de Recursos Financeiros Ltda. ("Navi Ventures"), Navi International - Administradora e Gestora de Recursos Financeiros Ltda. ("Navi Internacional"). Quando referidas em conjunto no presente documento, Navi Capital, Navi Yield, Navi Allocation, Navi Selection, Navi Ventures e Navi Internacional são designadas "Gestoras" ou "Grupo Navi".

O detalhamento do escopo das atividades de cada uma das Gestoras e regras para mitigação de conflitos de interesse pode ser consultado no Código de Ética do Grupo Navi.

Essa Política visa proteger as informações de propriedade e/ou sob guarda do Grupo Navi, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

2. Aplicabilidade

Essa política aplica-se a todos os Colaboradores, prestadores de serviços, sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento do Grupo Navi, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados das Gestoras tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

3. Objetivo

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética do Grupo Navi, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para as atividades das Gestoras.

Em atenção aos dispositivos da ICVM 558 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, o Grupo Navi procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

4. Premissas e Definições

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidencias, o que é de extremo valor para o Grupo Navi, dado o princípio fundamental de confiança que as Gestoras trabalham para manter junto aos seus clientes, o Grupo Navi utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança da ANBIMA, datado de dezembro de 2017.

O referido documento é um dos principias materiais sobre o tema no mercado financeiro, incluindo as melhores referências sobre proteção de dados.

Adiante, o Grupo Navi abordará os principais mecanismos e procedimentos de prevenção as ameaças ao patrimônio, à imagem e, principalmente, aos negócios das Gestoras.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de Compliance do Grupo Navi, sob a direção do Comitê de Riscos e Compliance do Grupo Navi.

Ademais, para implementação e monitoramento contínuo da presente Política, as Gestoras contam com o suporte e assessoria da empresa terceirizada de TI MDS Serviços Empresariais ("Múltipla-TI").

5. Programa de Segurança do Grupo Navi

(i) Identificação de Riscos:

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, de risco de imagem, danos financeiros ou perda de vantagem concorrencial, podendo tais danos serem irreparáveis.

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- Malware – softwares desenvolvidos para corromper computadores e redes:
    - Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
    - Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
    - Spyware: software malicioso para coletar e monitorar o uso de informações; e
    - Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
    - Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
    - Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
    - Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
    - Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
    - Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (distributed denial of services) e botnets - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (advanced persistent threats) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, as Gestoras podem estar sujeitas a mal funcionalidades dos sistemas utilizados e a atos/omissões de seus Colaboradores, que podem acarretar na perda e/ou adulteração de dados e Informações Confidenciais.

(ii) Ações de Prevenção e Proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para as Gestoras, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para o Grupo Navi, em caso de incidente de segurança.

Deste modo, faz parte da política de segurança do Grupo Navi segregar as informações geradas pelas Gestoras, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classifica-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) Green Flag:

- Quaisquer informações e/ou dados que as Gestoras tiveram acesso ou conhecimento por ser de domínio público (“Informação Pública”);
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) Yellow Flag:

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação).

c) Red Flag:

- Todas as Informações Confidenciais, a saber:
    - know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas

às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pelas Gestoras;

- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pelas Gestoras; e
- estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades das Gestoras e/ou de seus sócios e clientes.

A partir da definição acima, o Grupo Navi se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: Red Flag, Yellow Flag e Green Flag.

A partir desse ponto, passamos a mencionar os procedimentos de prevenção e proteção adotados pelas Gestoras:

1. Estrutura de TI

Para estabelecer os principais equipamentos, procedimentos e sistemas de Tecnologia da Informação do Grupo Navi, segue lista exemplificativa dos recursos das Gestoras:

- Desktops Dell, Lenovo, HP ou similar;
- Servidor na Nuvem;
- Nobreak com manutenção frequente e autonomia de 15 (quinze) minutos para todos os servidores e máquinas;
- Gerador a diesel no escritório principal para fornecimento de energia aos elevadores e ao escritório com autonomia de 08 (oito) horas, podendo ser reabastecido;
- 02 (dois) provedores de internet no escritório principal, sendo 01 (um) dedicado e failover;
- Firewall e proteção Fortigate;
- Backup diário do banco de dados e armazenamento das versões anteriores por 30 (trinta) dias e de fechamento de mês por 5 (cinco) anos;
- Backup em tempo real dos arquivos (Sharepoint) e armazenamento das versões em nuvem;
- Backup de imagem do servidor realizado em tempo real e Failover (site recovery Microsoft Azure);
- Antivírus Sophos em todos os computadores e servidores; entre outros programas que visam a salvaguarda dos dados;
- Entre outros.

Cabe salientar que as Gestoras possuem ambiente de acesso segregados, de modo que as diferentes áreas das Gestoras terão suas estruturas de armazenamento de informações logicamente segregadas das demais para garantir que apenas os Colaboradores autorizados e necessários para o desempenho de determinada atividade tenham acesso às informações da mesma.

Além dos recursos citados na lista, o Grupo Navi conta com o "Comitê Técnico" que é composto pelo Diretor de Compliance, o sócio responsável pelo BackOffice e dois coordenadores do time de BI/TI. Esse Comitê é responsável por definir a lista dos programas que podem ser instalados em cada máquina, liberar o uso de pen-drives de armazenamento em casos específicos, avaliar instalações de programas de fora da lista em casos de urgência, dentre outros pontos mencionados nos parágrafos a seguir. Caso haja qualquer dúvida de um dos membros do Comitê com relação a ação a ser realizada, o Diretor de Compliance deve ser consultado. O Comitê é uma das formas de atuação da área de Compliance.

2. Propriedade dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade do Grupo Navi. Não é permitida a utilização de notebooks, tablets ou outros hardwares pessoais para operações no âmbito das Gestoras, salvo mediante expressa permissão da área de Compliance.

3. Disponibilização e uso

Todos os computadores disponibilizados para os Colaboradores do Grupo Navi têm por objetivo o desempenho das atividades profissionais, não devendo ser utilizado para quaisquer outros fins.

Todo o processo de criação e exclusão de usuário, instalação de softwares e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela Múltipla-TI, mediante aprovação do Comitê Técnico.

A disponibilização e uso dos computadores das Gestoras respeitam as seguintes regras:

- A cada novo Colaborador, o Comitê Técnico autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos.
- Todos os equipamentos devem ser preparados e testados pela Multipla-TI, mediante supervisão e aprovação do Comitê Técnico.

- O Comitê Técnico autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário.
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da Múltipla-TI, mediante supervisão e aprovação do Comitê Técnico.
- A identificação do usuário é feita através do login e senha, com dupla autenticação, que através do registro de logs utilizado pelas Gestoras é sua assinatura eletrônica no ambiente das Gestoras.
- Será apenas permitida senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos.
- Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pelas Gestoras, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue.
- É permitido apenas 5 (cinco) tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação ao Comitê Técnico.
- Todos os eventos de login e alteração de senhas são auditáveis e rastreáveis.

4. Softwares

A implantação e configuração de softwares das Gestoras respeitam as seguintes regras:

- Todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela Múltipla-TI, mediante supervisão e aprovação do Comitê Técnico.
- É desabilitado aos usuários implantar novos programas ou alterar configurações.
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores.
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela gestora.
- A utilização de equipamentos pessoais por terceiros nas instalações das Gestoras e a conexão destes na rede interna à Internet requer autorização prévia e expressa do Comitê Técnico. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.
- A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia do Comitê Técnico.

5. Registros

As Gestoras mantêm logs de sistemas, e verificam regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados.

Nesse sentido, através dos logs realizados pelas Gestoras, consegue-se manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme 4º, §8º, da ICVM 558.

6. Responsabilidades do usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O Colaborador também deve garantir a integridade física dos equipamentos e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pelo Grupo Navi.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;
- Não transportar Informações Confidenciais do Grupo Navi em qualquer meio (CD, DVD, pendrive, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e
- Seguir corretamente as políticas para uso de internet e correio eletrônico estabelecidas conforme disposto na presente Política.

7. Outras Proteções aos Computadores

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente).

8. Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia do Grupo Navi, este deve sempre resguardar a imagem das Gestoras, evitando entrar em sites de fontes não seguras, ou, de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pela Área de Compliance.

O usuário é proibido de acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

9. Bloqueio de endereços de Internet

Periodicamente, o Comitê Técnico irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética do Grupo Navi.

10. Uso de correio eletrônico particular

É proibida a utilização profissional de correio eletrônico particular, a não ser em situação de contingência com a devida autorização do Comitê Técnico.

O Grupo Navi disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence às Gestoras. Esse endereço não deve ser usado em hipótese alguma para fins particulares.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com o Grupo Navi.

Se houver necessidade de troca de endereço, a alteração será realizada pela Múltipla-TI, mediante autorização e supervisão do Comitê Técnico.

11. Endereço eletrônico de programas ou de comunicação corporativa

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.
É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo comunicação interna das Gestoras.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade do Grupo Navi.

12. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pelas Gestoras mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico das Gestoras.

13. Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;

- Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem do Grupo Navi; e
- Sejam incoerentes com o Código de Ética do Grupo Navi.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico das Gestoras é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome do Grupo Navi.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado. O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
- Ao uso da opção Encaminhar (Forward), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

14. Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria o e-mail corporativo das Gestoras fica na nuvem de um reconhecido provedor desse tipo de serviço (Microsoft).

15. Armazenamento em Nuvem (Cloud)

As Gestoras realizarão o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (Cloud).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

16. Contratação de Terceiros para Serviços de Armazenamento na Nuvem

Fornecedores, prestadores de serviços e parceiros ("Terceiros") podem representar uma fonte significativa de riscos para o Grupo Navi em relação à Cibersegurança. Neste sentido, as Gestoras só poderão contratar serviços de nuvem de grandes empresas de tecnologia que devem ter os seus papéis listados em bolsa de valores e valor de mercado acima de R$100.000.000,00 (cem milhões de reais).

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos aos provedores destes serviços, tal como, porém, não exclusivamente:

(i) Software as a Service (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores;
(ii) Platform as a Service (PaaS) – desenvolvimento, teste, uso e controle sobre softwares próprios; e
(iii) Infrastructure as a Service (IaaS) – utilização e controles sobre softwares próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais.

Por fim, as Gestoras podem deixar de realizar os procedimentos aqui dispostos, desde que respeitada a previsão da Política de Seleção, Contratação e Monitoramento de Terceiros.

6. Monitoramento e Testes de Contingência

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela Múltipla-TI, sob supervisão do Comitê Técnico. O referido monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados periodicamente, de modo a permitir que as Gestoras estejam preparadas para a continuação de suas atividades, assim como para mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios do Grupo Navi.

7. Plano de Resposta

Conforme as melhores práticas de mercado, o Grupo Navi desenvolveu um Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política. Estas providências consistem em:

Empresa de TI Terceirizada (Sob Supervisão do Compliance):

a) Verificação e Auditoria dos Logs;
b) Criação de laudo pericial contendo as informações que foram potencialmente vazadas;
c) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;
d) Desinstalação de software;
e) Execução de varreduras offline para descobrir quaisquer ameaças adicionais;
f) Formatação e reconstrução do sistema operacional;
g) Substituição física de dispositivos de armazenamento
h) Reconstrução de sistemas e redes;
i) Restauração de dados provenientes do backup realizado diariamente;
j) Entre outros.

Compliance ou Jurídico Contratado:

a) Criação de relatório baseado no laudo pericial elaborado pela empresa de TI terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança;
b) Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido.

BackOffice:

a) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos das Gestoras.
b) Realizar planejamento de contenção de risco de liquidez frente à possibilidade de resgate de investimentos das Gestoras resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados pela área de Compliance, bem como ser formalizado no Relatório de Controles Internos das Gestoras.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética do Grupo Navi.

8. Vigência e Atualização

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/ME sob o nº _____, declaro que li e estou plenamente de acordo com as disposições da Política de Segurança da Informação e Segurança Cibernética aprovados pelo Grupo Navi em [●]. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

[Rio de Janeiro/São Paulo], [Data]

_____

[Assinatura]