POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

AZ GUIDANCE GESTÃO DE PATRIMÔNIO LTDA.

Fevereiro/2025 – Versão 1.0

ÍNDICE

INTRODUÇÃO

A AZ Guidance Gestão de Patrimônio Ltda. ("Gestora" ou "AZ Guidance") apresenta a sua Política de Segurança da Informação e Segurança Cibernética ("Política").

Esta política se aplica a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da AZ Guidance, ou que acessem informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da Gestora tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da AZ Guidance.

Em linha com as principais discussões e preocupações do mercado, a Política tem como base princípios e procedimentos que assegurem a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pela AZ Guidance.

OBJETIVOS

Esta Política tem por objetivo estabelecer regras e definir medidas para identificar e prevenir contingências, tanto informacional quanto cibernética, que possam causar prejuízo para a consecução das atividades da AZ Guidance.

Neste sentido, e em atenção aos dispositivos da Resolução CVM nº 21/21 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, procurou-se 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 atividade da Gestora.

PROGRAMA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

Definições

A Segurança Cibernética busca mecanismos de proteção e defesa voltados à prevenção de ataques maliciosos direcionados a sistemas, redes e programas, com o objetivo de mitigar eventuais danos, tanto em nível de hardware quanto de software.

Já a Segurança da Informação busca garantir a proteção de dados e informações contra acessos não autorizados, alterações indevidas, perda ou indisponibilidade. Seu principal objetivo é garantir três pilares fundamentais:

- Confidencialidade: somente pessoas devidamente autorizadas pela empresa deverão ter acesso às informações;
- Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações; e
- Disponibilidade: as informações devem estar disponíveis para as pessoas autorizadas, sempre que necessário.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da AZ Guidance, que não as necessitem, ou que não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a AZ Guidance, ou de qualquer natureza relativa às atividades da empresa e a seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser fornecida ao público, mídia ou a demais órgãos, caso autorizado pelo Diretor de Risco e *Compliance*.

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, *software*s 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

restabelecido.

- 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; e
- 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, a AZ Guidance pode estar sujeita à más funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar na perda e/ou adulteração de dados e Informações Confidenciais.

No âmbito das atividades realizadas pela AZ Guidance, os principais ativos identificados que precisam de proteção são:

- **Dados e Informações:** 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, suas ameaças possíveis e sua vulnerabilidade;
- **Equipamentos:** Servidores, *Switches*, *Firewall*, provedores de internet, *Desktops* e *Laptops*.

São consideradas Informações Confidenciais:

- *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 pela AZ Guidance;
- Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela AZ Guidance; e
- Estruturas, planos de ação, relação de clientes, contrapartes comerciais, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da AZ Guidance e/ou de seus sócios e clientes.

Ações de Prevenção e Proteção

Backups

A AZ Guidance armazena seus dados e informações confidenciais na Nuvem, em Datacenters de empresas terceirizadas com ambiente controlado e contingenciado, sendo possível o acesso mediante autenticação, em caso de necessidade. Os Datacenters possuem backup por período determinado, ou seja, se algum arquivo for apagado ou alterado de forma errônea ou maliciosa, é possível recuperá-lo neste período.

O sistema proprietário da AZ Guidance utiliza servidor provido por empresa de alta reputação, que possui Datacenters com ambientes controlados e contingenciados. Este servidor também conta com backup diário por período determinado, possibilitando a recuperação de arquivos em caso de necessidade.

Restrição de Acessos Físicos

A AZ Guidance conta com controle de acesso ao escritório, garantindo que apenas pessoas autorizadas adentrem às instalações da Gestora. Ademais, os recursos computacionais e de sistemas disponibilizados para os Colaboradores são mantidos em área considerada segura, com controle de acesso individualizado e passível de bloqueio.

A rede de comunicação de dados local possui acesso restrito.

Por fim, A AZ Guidance conta com sistema de segurança por videomonitoramento das instalações físicas com backup de vídeo, caso seja necessário a recuperação de imagens.

Acesso Remoto

A AZ Guidance permite o uso de acesso remoto, desde que seja realizado por meio de ferramenta que contenha criptografia e fatores de autenticação.

Os Colaboradores são instruídos a (i) manter softwares de proteção contra

malware/antivírus nos dispositivos remotos, (ii) relatar ao Diretor de Risco e Compliance qualquer 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 de qualquer natureza relativas às atividades da AZ Guidance em dispositivos pessoais.

Segregação de Redes

A Gestora possui segregação de redes, mantendo uma rede exclusiva para os Colaboradores da Gestora. Ademais, são disponibilizadas redes específicas para Assessores de Investimentos e Consultores. Por fim, a Gestora conta com rede segregada para clientes e visitantes, com acesso mediante login e senha disponibilizados pela AZ Guidance.

Antivírus e Firewall

A Gestora utiliza um hardware e um software de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas.

A Gestora mantém 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). São conduzidas varreduras periódicas para detectar e limpar qualquer ameaça em dispositivos da Gestora.

Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da AZ Guidance ou alugados de empresas especializadas. Não é permitida a utilização de notebooks, tablets ou outros hardwares fornecidos pela AZ Guidance para uso pessoal dos Colaboradores, salvo expressa permissão do Diretor de Risco e *Compliance*.

Regras de Uso dos Recursos de TI

Todos os computadores disponibilizados para os Colaboradores da AZ Guidance têm por objetivo o desempenho das atividades profissionais na AZ Guidance, 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 realizadas pela área responsável, mediante aprovação do Compliance.

É desabilitado aos usuários implantar novos programas ou alterar configurações, sem a permissão do Compliance

Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores que precisarem destas informações para realizar suas

atividades, observada a devida segregação de funções, e, após prévia autorização do Compliance. Ademais, haverá o cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na AZ Guidance.

A senha que foi fornecida para acesso à rede de dados institucionais não deverá, em nenhuma hipótese, ser revelada a outra pessoa, podendo o Colaborador ser responsabilizado caso disponibilize a terceiros tais senhas para quaisquer fins.

A disponibilização e uso dos computadores da AZ Guidance respeitam as seguintes regras:

- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela AZ Guidance;
- A cada novo Colaborador, será feita a criação de novo usuário e a disponibilização técnica de recursos, mediante supervisão do Compliance;
- Todos os equipamentos, *software*s e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão do *Compliance*;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento;
- A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela AZ Guidance é sua assinatura eletrônica no servidor da AZ Guidance;
- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da expiração da mesma;
- Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de Risco e *Compliance* à área responsável;
- A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia do Compliance.

As regras sobre senhas poderão ser modificadas a qualquer momento, em decorrência de avanços tecnológicos ou decisão interna da área de Compliance da AZ Guidance, visando sempre o aprimoramento dos procedimentos, sistemas e da segurança das informações.

A utilização de equipamentos pessoais por terceiros nas instalações da AZ Guidance e a conexão destes na rede interna à Internet requer autorização prévia do *Compliance*.

Todo conteúdo que está na rede pode ser acessado pela área de Compliance, caso haja necessidade. Os demais Colaboradores têm acessos previamente definidos.

Registros

A AZ Guidance mantém por 5 anos todos os *logs* de sistemas, e verifica 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 pela AZ Guidance, a gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme Resolução CVM nº 21/21.

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 sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela AZ Guidance.

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 da AZ Guidance 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 contenham Informações Confidenciais; e
- Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela AZ Guidance.

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);
- "Log-*off*" automático por inatividade durante o período de 24 horas;
- Bloqueio do acesso às portas *USB* dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores.

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 da AZ Guidance, este deve sempre resguardar a imagem da AZ Guidance, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails pessoais, ou, de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo *Compliance*.

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

- Possam violar direitos de autor, marcas, licenças de programas (*software*s) ou patentes existentes;
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
- Contenham informações que não colaborem para o alcance dos objetivos da AZ Guidance;
- 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.

Também se faz expressamente proibido o uso de serviços de rádio, streaming, download de vídeos, filmes e músicas, que não sejam relacionados com a atividade profissional, através dos computadores da AZ Guidance.

<u>Uso de Correio Eletrônico Particular</u>
É proibido a utilização profissional de correio eletrônico particular.

A AZ Guidance disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@azguidance.com.br)

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à AZ Guidance.

<u>Acesso à Distância ao E-mail</u>
O usuário pode acessar o seu correio eletrônico cedido pela AZ Guidance 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 como se estivesse no ambiente físico da AZ Guidance.

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, podendo enviar mensagens necessárias para o seu desempenho profissional na AZ Guidance.

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;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a AZ Guidance, a sugestão deve ser encaminhada para a área de Compliance, que definirá a sua publicação ou não;
- 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 suscetíveis 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 da AZ Guidance; e
- Sejam incoerentes com o Código de Ética e Conduta da AZ Guidance.

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 da AZ Guidance 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 da AZ Guidance.

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.

Cópias de Segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria, a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área responsável.

Armazenamento em Nuvem (*Cloud*)

A AZ Guidance poderá realizar 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.

Contratação de Terceiros para Serviços de Armazenamento na Nuvem

Fornecedores, prestadores de serviços e parceiros ("Terceiros") podem representar uma fonte significativa de riscos para a AZ Guidance em relação à Cibersegurança e segurança da informação. Assim, todos os Terceiros a serem contratados pela AZ Guidance devem passar por *Due Diligence*, sendo verificado o conteúdo mínimo do Anexo II desta Política, além de avaliar os controles de segurança na própria estrutura dos terceiros e outras exigências da Política de Seleção e Contratação de Terceiros. Ademais, quando da contratação, deverão assinar o termo de adesão à presente Política, conforme o Anexo I, ou possuir nos contratos de prestação de serviços cláusula de confidencialidade.

Quanto à contratação de Terceiros para serviços de Armazenamento na Nuvem, é necessário se adotar certos procedimentos específicos, como os descritos adiante. Será necessário iniciar um devido processo de *Due Diligence* do Terceiro antes da contratação, devendo-se constatar se a organização segue políticas, programas e procedimentos formais relativos à segurança da informação e Cibersegurança.

Somente após a aprovação pela área de *Compliance*, o Terceiro poderá ser contratado para prestar serviços de Armazenamento na Nuvem.

Em caso de qualquer incidente constatado pelo Terceiro, este deverá de imediato enviar uma notificação relatando o ocorrido à AZ Guidance, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos de *Due Dilligence* 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 *software*s próprios; e
(iii) Infrastructure *as a Service* (IaaS) – utilização e controles sobre *software*s próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais.

Monitoramento e Testes Periódicos

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela área responsável, sob supervisão do *Compliance*. O referido monitoramento acontecerá de forma contínua e adotará uma abordagem intensificada de acordo com o nível de risco a que os sistemas e informações digitais da AZ Guidance estão expostos, conforme procedimentos descritos nessa Política.

A AZ Guidance, através da empresa de TI contratada, monitora diariamente a realização de backups dos seus arquivos e redes.

A empresa contratada de TI também é responsável por manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

Ademais, para o monitoramento dos controles, os inventários de *hardware* e *software* são mantidos e atualizados.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a AZ Guidance esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da AZ Guidance.

Ademais, serão realizados Testes Periódicos de Segurança, com especial enfoque no plano de resposta a incidentes. Referidos testes serão realizados anualmente pela empresa de TI terceirizada e o resultado será consolidado no relatório anual de controles internos da AZ Guidance.

Plano de Resposta

Conforme as melhores práticas de mercado, a AZ Guidance 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 da Companhia;

b) Realizar planejamento de contenção de risco de liquidez frente à possibilidade de resgate de investimentos da AZ Guidance 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 da AZ Guidance.

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

DISPOSIÇÕES GERAIS

Para elaboração desta Política foi utilizada a 3ª edição do Guia de Cibersegurança ANBIMA. O referido documento é um dos principais materiais sobre o tema no Mercado Financeiro, incluindo as melhores referências sobre proteção de dados.

Ademais, para implementação e monitoramento contínuo da presente Política, a AZ Guidance conta com o suporte e assessoria da empresa terceirizada de TI, sob supervisão do *Compliance*.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada periodicamente, pelo menos 01 (uma) vez ao ano, 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 demandarem tal providência.

O objetivo principal do processo de revisão dessa Política é manter sempre atualizada a metodologia de avaliação de risco, as implementações de proteção e prevenção, os monitoramentos e testes e os planos de resposta.

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1	Fevereiro/2024	AZ Guidance	Versão inicial
2	Fevereiro/2025	AZ Guidance	Revisão geral da Política

ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Nesta data, eu, _____, inscrito no [CPF/ME ou CNPJ] sob o nº _____ , declaro que li e estou plenamente de acordo com as disposições da Política de Segurança da Informações e Segurança Cibernética da AZ Guidance Gestora de Recursos Ltda. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

Rio de Janeiro, [Data]

_____

[Assinatura]

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

Conteúdo mínimo de Compliance em segurança cibernética a ser verificado pelo Compliance:

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?
Resposta:

2. A empresa apresenta plano de resposta a incidentes de cibersegurança?
Resposta:

3. A empresa apresenta ações de conscientização, educação e formação de segurança da informação junto a seus funcionários?
Resposta:

4. Quais são as ferramentas e os mecanismos utilizados para proteção de dados transacionados com a empresa contratante?
Resposta:

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.
Resposta:

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 clientes e/ou reguladores (quando aplicável)?
Resposta:

Favor disponibilizar os seguintes documentos:
- 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.
- Certificações: solicitar envio de certificações que possam comprovar a devida capacidade técnica do prestador de serviço.