POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Guidance Gestora de Recursos Ltda.

Fevereiro/2023 – Versão 1.0

ÍNDICE

APRESENTAÇÃO 3
OBJETIVOS 3
PREMISSAS E DEFINIÇÕES 4
PROGRAMA DE SEGURANÇA DA GUIDANCE 4
MONITORAMENTO E TESTES PERIÓDICOS 16
PLANO DE RESPOSTA 17
VIGÊNCIA E ATUALIZAÇÃO 18
ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA 20

APRESENTAÇÃO

A Política de Segurança da Informação e Segurança Cibernética ("Política") da Guidance Gestora de Recursos Ltda. ("Guidance"), aplica-se a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Guidance, ou que acessem informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da 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 Guidance.

OBJETIVOS

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Guidance, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

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, a Guidance 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 a sua atividade.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada à pessoas, dentro ou fora da Guidance, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais. Com o propósito de manter a confidencialidade das informações, bem como garantir a integridade e disponibilidade destas, a Guidance leva em consideração três aspectos básicos, quais sejam:

- 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.

Qualquer informação sobre a 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*.

PREMISSAS E DEFINIÇÕES

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidenciais, o que é de extremo valor para a Guidance, dado o princípio fundamental de confiança que a instituição trabalha para manter junto aos seus clientes, a Guidance 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 principais materiais sobre o tema no Mercado Financeiro, incluindo as melhores referências sobre proteção de dados.

Adiante, a Guidance abordará os principais mecanismos e procedimentos de prevenção às ameaças ao patrimônio, à imagem e, principalmente, aos seus negócios.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de *Compliance* da Guidance, sob a direção do Diretor de Risco e *Compliance* da instituição.

Ademais, para implementação e monitoramento contínuo da presente Política, a Guidance conta com o suporte e assessoria da empresa terceirizada de TI.

PROGRAMA DE SEGURANÇA DA GUIDANCE

(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, *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.

A Guidance deve, ainda, identificar todos os ativos relevantes da instituição (sejam equipamentos, sejam sistemas, processos ou dados) usados para o correto funcionamento das atividades. As vulnerabilidades dos ativos identificados devem ser avaliadas, identificando as possíveis ameaças e o grau de exposição dos ativos a elas.

Diferentes cenários devem ser considerados nessa avaliação. O processo de avaliação de riscos deve contemplar as atividades desenvolvidas por prestadores de serviços terceirizados, incluindo, mas não se limitando, aos serviços de nuvem.

Ainda, além de ataques cibernéticos, a Guidance pode estar sujeita à más funcionalidades dos sistemas utilizados e a atos ou omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

(ii) <u>Ações de Prevenção e Proteção</u>

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

Deste modo, a Guidance segrega as informações geradas pela instituição, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações. Dessa forma, é possível providenciar maior proteção às informações digitais que possuem maior risco, como, mas sem se limitar, restringindo o acesso físico das áreas que mantêm Informações Confidenciais.

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

a) *Green Flag:*

- Quaisquer informações e/ou dados que a Guidance teve 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 pela Guidance;
- operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Guidance; 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 da Guidance e/ou de seus sócios e clientes.

A partir da definição acima, a Guidance se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo 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 pela Guidance:

<u>Estrutura de TI</u>

Os principais equipamentos, procedimentos e sistemas de Tecnologia da Informação da Guidance são:

- Backup diário local e externo – via Dropbox e Servidor;
- 1 Switch Gigabit Ethernet HPE Office Connect 48, 1 Roteador cisco (cedido pela empresa de Internet – Mundivox) /Firewall Fortinet;
    - 1 (um) link de Internet Dedicado – 50MB - Mundivox; e
    - 1 (um) link de Internet Dedicado – 10MB - Embratel.
- 1 multifuncional Canon C3525i (impressão, cópia e digitalização)
- 1 Linhas de telefone digitais – Embratel - 01 Gateway de E1, para comunicação com o PABX central de São Paulo;

- Computadores corporativos com acesso à Internet, todos com extensão de garantia de hardware;
    - 6 estações de trabalho Dell;
    - 4 estações de trabalho HP;
    - 3 notebooks (2 Lenovos e 1 Dell).
- Acesso ao sistema de informações de posição dos fundos e gerenciamento de riscos;
- Sistema de Firewall com sistema de detecção de invasão – VPN corporativa com acessos auditados. Contempla um sistema de Web Filtro (limita os acessos);
- Sistema de correio eletrônico com anti-spam e recursos de regras para controle de envio de e-mails – Microsoft Exchange;
- Nobreak com gerenciamento para prevenção de surtos elétricos e estabilização elétrica de todas as tomadas dos equipamentos sensíveis da empresa, como Switch, Servidor e Firewall;
- CPD local e com acesso restrito à área.

I. Propriedade dos Recursos de TI

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

II. Disponibilização e uso

Todos os computadores disponibilizados para os Colaboradores da Guidance têm por objetivo o desempenho das atividades profissionais na 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 Diretor de Risco e 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 Diretor de Risco e Compliance. Ademais, haverá o cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na 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 Guidance respeitam as seguintes regras:

- A cada novo Colaborador, o Diretor de Risco e *Compliance* autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos, *software*s e permissões acessos devem ser testados, homologados e autorizados pela área responsável, mediante supervisão e aprovação do Diretor de Risco e *Compliance*;
- O Diretor de Risco e *Compliance* 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 área responsável, mediante supervisão e aprovação do Diretor de Risco e *Compliance*;
- A identificação do usuário é feita através do *login* e senha, que através do registro de *logs* utilizado pela Guidance é sua assinatura eletrônica no servidor da Guidance;
- Será apenas permitida senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 05 (cinco) vezes;
- Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela Guidance, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue;
- É permitida apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação ao Diretor de Risco e *Compliance*.
- 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.

As regras sobre senhas poderão ser modificadas a qualquer momento, em decorrência de avanços tecnológicos ou decisão interna da área de

Compliance da Guidance, visando sempre o aprimoramento dos procedimentos, sistemas e da segurança das informações.

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

III. Softwares

A implantação e configuração de *software*s da Guidance respeitam as seguintes regras:

- Todos os *software*s, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área responsável, mediante supervisão e aprovação do Diretor de Risco e *Compliance;*
- É desabilitado aos usuários implantar novos programas ou alterar configurações, sem a permissão formalizada do Diretor de Risco e *Compliance*;
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores;
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Guidance;
- A utilização de equipamentos pessoais por terceiros nas instalações da Guidance e a conexão destes na rede interna à Internet requer autorização prévia e expressa do Diretor de Risco e *Compliance*. 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 e expressa do Diretor de Risco e *Compliance*.

IV. Registros

A Guidance mantém por 5 anos todos os *logs* de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam *software*s, *hardwares* ou acessos que não sejam autorizados.

Nesse sentido, através dos logs realizados pela Guidance, a gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme Resolução CVM nº 21/21.

V. 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 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 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 Guidance.

VI. 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 as portas *USB* dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores;
- Bloqueio do acesso a sites de armazenamento de dados em Nuvem (*Cloud*);
- Bloqueio de sistemas de gerenciamento de computador à distância.

VII. 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 Guidance, este deve sempre resguardar a imagem da 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 Diretor de Risco e *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 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, através dos computadores da Guidance.

VIII. Bloqueio de endereços de Internet

Periodicamente, a Área de *Compliance* irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Guidance.

IX. Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular.

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

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

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

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Risco e *Compliance*.

X. 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 da Área de *Compliance* 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 da Guidance, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a este correio eletrônico são de propriedade da Guidance.

XI. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela 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 Guidance.

XII. 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 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 Guidance, a sugestão deve ser encaminhada para a Área de Recursos Humanos, 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 Guidance; e
- Sejam incoerentes com o Código de Ética Corporativa da 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 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 Guidance.

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.

XIII. 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, mediante supervisão do Diretor de Risco e *Compliance*.

XIV. Armazenamento em Nuvem (*Cloud*)

A 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.

XV. 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 Guidance em relação à Cibersegurança e segurança da informação. Assim, todos os Terceiros a serem contratados pela 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 Pólítica 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.

Com isto em mente, a empresa objeto de contratação deverá enviar a Guidance:

(i) Documentos que atestem a existência dos respectivos procedimentos de Cibersegurança;
(ii) Último relatório de teste/auditoria periódica;
(iii) As certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

Uma vez recebidos os respectivos documentos, a Área de *Compliance* analisará o Terceiro, podendo negar de imediato a contratação deste ou exigir remediações para que este se encaixe nos moldes de segurança a serem aplicados pela Guidance.

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 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 Diretor de Risco e *Compliance*. O referido monitoramento acontecerá de forma contínua e adotará a abordagem baseada em risco intensificado; assim, de acordo com o nível de risco a que os sistemas e informações digitais da Guidance estão expostos, conforme procedimentos descritos nessa Política.

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

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 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 Guidance.

Ademais, serão realizados Testes Periódicos de Segurança a Guidance, com especial enfoque em segregação lógica, testes de penetração, resposta a eventos de vazamento de dados, rastreabilidade dos logs de acessos às informações sensíveis, tratamento de dados, dentre outros, sempre objetivando a preservação dos dados mantidos pela Guidance, em especial os confidenciais. Referidos testes serão realizados, com periodicidade mínima semestral, pela empresa de TI terceirizada e o resultado será consolidado no relatório anual de controles internos da Guidance.

PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a 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:

<u>Empresa de TI Terceirizada (Sob Supervisão do *Compliance*):</u>

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 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 Guidance.

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

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/2023	Guidance	Versão inicial

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 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

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.