MANUAL DE CONFORMIDADE (*COMPLIANCE*) E CONTROLES INTERNOS

DA

GUEX CONSULTORIA DE VALORES MOBILIÁRIOS LTDA.
CNPJ: 53.063.062/0001-09

ATUALIZADO EM DEZEMBRO DE 2023

MANUAL DE CONFORMIDADE (COMPLIANCE) E CONTROLES INTERNOS

Manual de Conformidade (*Compliance*) e Controles Internos ("**Manual**") da Guex Consultoria de Valores Mobiliários Ltda., sociedade empresária limitada, inscrita no CNPJ sob o nº 53.063.062/0001-09, com sede na cidade do Rio de Janeiro, Estado do Rio de Janeiro, na Av. Afrânio de Melo Franco nº 290, sala 408 (parte), Leblon, CEP: 22430-060.

I. INTRODUÇÃO

Este Manual estabelece as diretrizes e normas que são mandatórias para todos os "**Colaboradores**" da Guex, assim denominados os: (i) sócios; (ii) funcionários; e (iii) quaisquer pessoas que possuam cargos, funções ou posições na Guex. O propósito deste Manual é definir os procedimentos, as normas de Compliance e os controles internos da Guex, incluindo aspectos como confidencialidade e segregação de atividades. Este Manual foi elaborado de acordo com os requisitos estabelecidos pela Comissão de Valores Mobiliários ("**CVM**").

O programa de Compliance da Guex é destinado a instituir, bem como a manter atualizados e efetivos, os controles internos, em linha com a complexidade das atividades desenvolvidas. O objetivo é garantir conformidade (Compliance) contínua com as leis e regulamentações em vigor.

Em consonância com a sua política interna, a Guex espera que cada um de seus Colaboradores execute seu trabalho de maneira ética, legal e honesta, respeitando sempre o dever fiduciário devido aos clientes, potenciais clientes e outros participantes do mercado.

II. ESTRUTURA ORGANIZACIONAL

Alta Administração da Guex

A Alta Administração, conforme conceito dado pela Res. CVM 50, é o órgão decisório máximo da Guex, responsável pelos assuntos estratégicos da Guex, pela atividade de consultoria de valores mobiliários e pelo cumprimento de regras, políticas, procedimentos e controles da Guex, comprometendo-se com a efetividade e adequação da presente Política PLD/FTP e demais políticas, manuais, protocolos e dos controles internos da Guex.

Os membros da Alta Administração são profissionais com profunda expertise e competência técnica, responsáveis pela eleição da Diretoria da Guex, incluindo o Diretor de Compliance que tem a responsabilidade de estabelecer diretrizes para prevenir a Lavagem de Dinheiro e Financiamento ao Terrorismo (LDFT) na Consultoria de Valores Mobiliários.

A Alta Administração é formada pelas Sras. (i) ANA PAOLA ANTUNES MACIEL GUETTA; e (ii) PATRÍCIA BARBOSA VIANA BITTENCOURT; (iii) RAFAEL DUARTE GOLDENSTEIN; e (iv) ADRIANO DA SILVA.

Diretor de Compliance – responsável pela PLD/FTP

O diretor indicado pela Guex para ser o responsável pela PLD/FTP, inclusive perante a CVM, é o Sr. **ADRIANO DA SILVA** ("**Diretor de PLD/FTP**"). O Diretor de PLD/FTP tem total independência, autonomia e conhecimento para o pleno cumprimento dos seus deveres, assim como tem pleno acesso a todas as informações que julgar necessárias para que a respectiva governança de riscos, bem como autonomia para garantir o exercício da Política PLD/FTP pela Guex.

As atribuições essenciais do Diretor de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FTP) incluem: (i) atuar como ponto de contato principal para todas as consultas internas e externas relacionadas ao PLD/FTP; (ii) supervisionar a estrutura de procedimentos e controles estabelecidos pela Guex; (iii) informar ao Conselho de Controle de Atividades Financeiras (COAF) em até 24 horas sobre transações ou propostas de transação que possam indicar a ocorrência de crimes de lavagem de dinheiro ou ocultação de bens, direitos ou valores provenientes, direta ou indiretamente, de infrações penais.

São atribuições do Diretor de Compliance:

a. Monitorar e auditar o programa de Compliance da Guex de forma periódica, bem como preservar registros e evidências dessas auditorias;

b. Manter e revisar o presente Manual, o Código de Ética, além das demais políticas internas da Guex;

c. Disponibilizar uma cópia atualizada deste Manual no site da Guex e fornecer uma cópia para cada Colaborador anualmente e sempre que houver atualizações;

d. Garantir a obtenção do Formulário 'Conheça seu Colaborador' da Guex, seja diretamente ou por meio de terceiro competente;

e. Coordenar a formação interna em Compliance, assegurando que esteja sempre atualizada de acordo com as leis e regulamentações pertinentes;

f. Coordenar e acompanhar quaisquer inspeções regulatórias;

g. Receber e responder prontamente a todas as perguntas e dúvidas dos Colaboradores sobre Compliance;

h. Registrar a conformidade de cada Colaborador com as políticas internas da Guex, bem como com as leis e regulamentações aplicáveis;

i. Comunicar quaisquer irregularidades à Alta Administração da Guex e aos órgãos reguladores competentes, quando pertinente;

j. Assegurar a correta guarda das evidências de análises de Compliance, que possam ser

pertinentes para futuras auditorias e inspeções regulatórias;

k. Elaborar o Relatório Anual de Compliance ("Relatório"). O Relatório, uma vez concluído, será apresentado à Alta Administração da Guex, contendo as seguintes considerações;

- conclusões dos exames efetuados;

- propostas de correções para eventuais falhas identificadas, com o respectivo cronograma para solução destas, se for o caso; e

- obter a opinião do diretor consultor de valores mobiliários, sobre as deficiências constatadas nas verificações e as ações planejadas de acordo com cronograma específico ou as medidas já adotadas para resolvê-las.

Respeitando as normas aplicáveis, o Diretor de Compliance tem a prerrogativa de delegar algumas responsabilidades e obrigações de compliance para outros Colaboradores, desde que devidamente qualificados e sempre em conformidade com a legislação pertinente.

O Diretor de Compliance detém plena autonomia e independência em suas decisões, sendo capaz de questionar os riscos assumidos nas operações realizadas e aplicar as devidas sanções disciplinares, independente de nível hierárquico, sem a necessidade de validação prévia dos administradores ou sócios da Guex.

III. CONFLITOS DE INTERESSE E PRESENTES

Política de Conflitos de Interesse

Este Manual estabelece a Política de Conflitos de Interesse, cujo objetivo é gerenciar, mitigar e, quando possível, eliminar todos os conflitos de interesse reais ou potenciais que possam surgir das atividades da Guex e de seus Colaboradores.

Os conflitos de interesse podem surgir quando um ou mais Colaboradores estão envolvidos em atividades ou relações que possam ser incompatíveis, em algum grau, com esta Política. Nestas situações, as condutas dos Colaboradores e as decisões de investimento podem entrar em conflito com suas funções na Guex, comprometendo sua capacidade de julgamento ou a eficácia de suas atividades profissionais. Portanto, o Colaborador deve exercer discernimento antes de se envolver em qualquer atividade ou transação que possa causar um conflito de interesse.

Na execução de suas atividades, a Guex e seus Colaboradores se comprometem a permanecer vigilantes e evitar situações em que seus interesses pessoais ou de terceiros possam entrar em conflito ou parecer contrários aos interesses da Guex ou de seus clientes.

Se um conflito de interesse se tornar inevitável, cabe ao Diretor de Compliance avaliar o conflito de interesse em questão e tomar as medidas necessárias para minimizar seus riscos. Qualquer conflito que não possa ser prevenido ou evitado deve ser imediatamente comunicado ao Diretor

de Compliance por qualquer Colaborador que o identifique.

Em último caso, Diretor de Compliance convocará uma reunião com a Alta Administração da Guex para deliberar sobre os conflitos de interesse.

São exemplos de possíveis conflitos de interesse:

• Um Colaborador (ou um parente próximo) ser proprietário ou administrador de uma empresa que negocia diretamente com a Guex;

• Um Colaborador ter um emprego ou interesses comerciais externos que possam interferir em sua capacidade de desempenhar seu trabalho na Guex;

• Um Colaborador (ou um parente próximo) ter influência significativa como acionista, diretor, funcionário, consultor ou agente de uma empresa, organização ou entidade concorrente da Guex ou que tenha negócios atuais ou futuros, seja como cliente, fornecedor ou contratado da Guex.

Os Colaboradores estão proibidos de utilizar de forma indevida informações, conhecimentos ou quaisquer outros recursos que sejam de propriedade da Guex. Se um Colaborador desejar exercer atividades externas, remuneradas ou não, deve comunicar previamente o Diretor de Compliance para obter sua aprovação, a fim de evitar possíveis conflitos de interesse e comprometimento de sua dedicação ao trabalho na Guex.

Comunicação e Aceite do Cliente em Situações de Conflito de Interesse

A transparência na relação com nossos clientes é fundamental para a Guex. Quando for identificada uma situação que possa caracterizar um conflito de interesse, é imperativo que os clientes afetados sejam informados prontamente.

Processo de Comunicação:

Assim que um potencial conflito for identificado e avaliado pelo Diretor de Compliance, a Guex enviará uma comunicação escrita aos clientes envolvidos. Esta comunicação descreverá claramente a natureza do conflito, suas implicações e as medidas propostas para gerenciá-lo ou mitigá-lo.

Aceite do Investidor:
Junto à comunicação, será enviada uma forma de aceite, na qual o cliente poderá manifestar sua concordância ou discordância em relação ao potencial conflito. O cliente terá um prazo determinado para responder que não poderá ser inferior a 5 (cinco) dias úteis. Caso não haja manifestação dentro deste prazo, entenderemos como aceite tácito.

Em situações em que o cliente manifeste discordância, a Guex buscará alternativas para resolver a situação, priorizando sempre os melhores interesses do cliente.

Registro de Comunicações e Aceites:
Todas as comunicações enviadas e os aceites recebidos, sejam eles explícitos ou tácitos, serão devidamente registrados e arquivados pela Guex, assegurando a rastreabilidade e a possibilidade de revisão futura.

3.1. Presentes, Brindes e Entretenimento

Os Colaboradores da Guex estão expressamente proibidos de receber qualquer forma de vantagem (como presentes, doações e brindes) de clientes, potenciais clientes, fornecedores e quaisquer terceiros que possam influenciar suas decisões ou ações dentro da Guex.

Em geral, os Colaboradores são proibidos de solicitar e desencorajados a aceitar presentes de clientes, potenciais clientes ou parceiros que não sejam membros de suas famílias, a menos que o valor desses presentes não exceda R$ 500,00 (quinhentos reais). Caso o valor seja maior, a situação deve ser analisada e decidida pelo Diretor de Compliance.

Está expressamente proibido para os Colaboradores oferecer, prometer dar, receber ou prometer receber, em nome da Guex, qualquer objeto de valor a qualquer colaborador de empresa atuante no mercado financeiro e de capitais ou órgãos reguladores, com a intenção de corrupção pública ou privada.

Ressaltamos que qualquer exceção a esta política, especialmente em relação à regra de R$ 500,00, deve ser claramente documentada e aprovada pelo Diretor de Compliance. A violação destas diretrizes poderá resultar em sanções disciplinares, incluindo a possibilidade de demissão e/ou desligamento do Colaborador.

3.1.1. Exceções.

Os brindes promocionais personalizados com a identificação do fornecedor ou cliente estão excluídos dessas normas. Refeições ocasionais e brindes de valor razoável também podem estar isentos dessas normas. Em caso de dúvida, o Colaborador deve buscar a aprovação do Diretor de Compliance.

Para esclarecer, as refeições realizadas durante uma reunião, seja na sede da Guex ou em outro local, não serão consideradas presentes, mas despesas de representação.

IV. POLÍTICA DE TREINAMENTO

O presente Manual dispõe sobre a política de treinamento de Compliance ("**Política de Treinamento de Compliance**"), que tem como objetivo estabelecer as condições, a frequência e a importância da realização de treinamentos junto aos Colaboradores da Guex.

O Diretor de Compliance da Guex é encarregado de organizar, ou garantir a organização, de treinamentos, anuais e obrigatórios, de Compliance, observados os seguintes temas:

- Prevenção à Lavagem de Dinheiro;
- Anticorrupção e Confidencialidade;

- Práticas de mercado, produtos disponíveis e regulamentação aplicável; e

- Insider Trading.

Os treinamentos serão disponibilizados aos Colaboradores de diversas formas, como acesso online, palestras presenciais, seminários ou materiais escritos. Esses treinamentos podem ser desenvolvidos e realizados por Colaboradores capacitados ou por escritórios de advocacia/terceiros qualificados contratados pela Guex.

O Diretor de Compliance deve manter, ou delegar a responsabilidade de manter, o registro de todos os treinamentos realizados, incluindo os materiais utilizados e a lista de Colaboradores que participaram e concluíram os treinamentos no tempo estipulado. A não conclusão dos treinamentos pode resultar em medidas disciplinares.

Todo novo Colaborador da Guex deverá receber ou ter acesso a todos os manuais, políticas e procedimentos internos da Guex, que passarão a fazer parte de suas atividades diárias.

V. POLÍTICA DE CONFIDENCIALIDADE

O presente Manual dispõe sobre a política de confidencialidade ("**Política de Confidencialidade**"), que tem como objetivo estabelecer os termos da confidencialidade das informações da Guex e seus clientes.

A confidencialidade é um dos princípios norteadores das atividades desenvolvidas dentro do mercado financeiro e de capitais. O princípio da confidencialidade deverá reger e será aplicável a todas e quaisquer informações (i) não públicas da Guex, (ii) obtidas pela Guex no curso de suas atividades, e (iii) recebidas de clientes, ex-clientes ou potenciais clientes ("**Informações Confidenciais**").

Inclui-se na definição de Informações Confidenciais todas as comunicações orais e escritas, informais ou não, independentemente do meio enviado, seja presencialmente, por carta, impressão, correio eletrônico, assim como a informações geradas no computador ou aplicativo de comunicação.

Os Colaboradores da Guex deverão proteger a confidencialidade das Informações Confidenciais que não sejam de domínio público, informações essas que tenham obtido ou criado em função das atividades que desempenham ou desempenharam junto à Guex.

Nenhum Colaborador poderá revelar qualquer Informação Confidencial ou informação proprietária referentes à Guex, seus Colaboradores, clientes, ex-clientes, clientes em potencial ou parceiros, a terceiros que não estejam autorizados a recebê-las ou sobre as quais não tenham necessidade de tomar conhecimento.

A única exceção é a revelação autorizada pelo cliente ou parceiro, ou requerida por lei ou autoridade competente, como por exemplo, os órgãos fiscalizadores de supervisão, em processo

legal cabível.

Acessos Remotos:
O acesso remoto aos sistemas da Guex só é permitido através de uma conexão segura VPN (Virtual Private Network) ou outros mecanismos similares de proteção.

Apenas colaboradores autorizados podem realizar acessos remotos e devem utilizar dispositivos de segurança (tokens) e autenticação em dois fatores.

Todos os acessos remotos devem ser registrados e monitorados pelo departamento de Compliance.

Uso de Dispositivos Móveis:
Os colaboradores devem utilizar dispositivos móveis fornecidos e gerenciados pela Guex para acessar informações confidenciais.

O uso de dispositivos pessoais para acessar sistemas da empresa é proibido, a menos que estejam em conformidade com as políticas de segurança da Guex e sejam previamente aprovados pelo departamento de Compliance.

Uso de Plataformas de Comunicação Externas:
Todos os documentos e comunicações envolvendo informações confidenciais devem ser realizados através de plataformas e sistemas fornecidos e monitorados pela Guex.

Formação e Conscientização:
Todos os colaboradores da Guex devem passar por treinamentos regulares sobre a importância da segurança da informação e as consequências de violações das políticas estabelecidas.

Violações:
Qualquer violação dessas regras resultará em ações disciplinares, que podem incluir a rescisão do contrato de trabalho e/ou o desligamento da Sociedade.

A Guex reserva-se o direito de monitorar e revisar qualquer informação transmitida ou recebida através de seus sistemas para garantir a conformidade com suas políticas.

Comunicação de Incidentes:
Todos os colaboradores têm a obrigação de comunicar imediatamente ao departamento de Compliance qualquer suspeita ou confirmação de vazamento ou comprometimento de informações confidenciais.

A Guex está comprometida em proteger todas as informações confidenciais, reservadas ou privilegiadas e espera que seus colaboradores façam o mesmo. A cooperação total é essencial para garantir a segurança da informação e a conformidade com todas as regulamentações aplicáveis.

Proteção das Informações de Clientes.

A Guex e os seus Colaboradores reconhecem a sua obrigação de resguardar as informações recebidas ou que se refiram aos seus clientes de forma segura e confidencial.

É um compromisso da Guex manter seguras as informações e usá-las de modo adequado, que preza pela confiança de seus clientes e Colaboradores.

Os Colaboradores também devem garantir que as informações recebidas sejam utilizadas apenas para as finalidades para as quais foram colhidas, salvo se outro tipo de utilização for permitido por lei ou normas internas.

Informações pessoais confidenciais somente poderão ser compartilhadas: (i) dentro da Guex e quando seja necessária para a condução de seus negócios; (ii) com as afiliadas da Guex e outras empresas, quando necessário e permitido pela legislação aplicável para atender o cliente; e (iii) com os reguladores e/ou quando exigido por lei, norma, regulamentos ou ordem judicial emitida por um tribunal de jurisdição competente, ou por um órgão, judiciário, administrativo ou legislativo; desde que, no entanto, o Diretor de Compliance seja consultado previamente para aprovação.

Quaisquer outras exceções para o compartilhamento de Informações Confidenciais, com pessoas não autorizadas, deverão ser revisadas e previamente aprovadas pelo Comitê de Risco e Compliance.

Informações sobre a Guex deverão ser disponibilizadas apenas se tiverem um propósito legítimo da sociedade. O compartilhamento de informações deve ser restrito e deverá ser feito com o entendimento de que as mesmas são confidenciais e devem ser utilizadas exclusivamente para o objeto restrito para o qual foram recebidas ou concedidas.

A Informação Confidencial só pode ser usada para fins profissionais e sob nenhuma hipótese deve ser utilizada para obtenção de quaisquer vantagens pessoais. É estritamente proibida a divulgação de informação para terceiros não envolvidos ou não autorizados a recebê-la.

O serviço de e-mail da Sociedade se encontra na nuvem, através da solução Office 365 Business da Microsoft e seu ambiente interno é garantido por dispositivo de segurança que executa funções de firewall e antivírus no nível do roteador. Além disso, uma proteção contra vírus é ativada em cada computador individual na rede de escritório. Com seus procedimentos de backup externo e acesso remoto a e-mails, a mesma pode continuar a funcionar mesmo que não possa ter acesso físico ao escritório. O backup externo é realizado por soluções da Microsoft.

VI. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Este Manual estabelece a Política de Segurança da Informação ("**Política de Segurança da Informação**"), que orienta todos os colaboradores da Guex. Seu principal objetivo é garantir a proteção de todas as informações significativas acessadas pelos colaboradores devido às suas funções ou cargos na empresa. Além disso, zela pela segurança das informações, incluindo aquelas armazenadas ou acessíveis nos equipamentos fornecidos pela Guex para desempenho de suas funções. Cada colaborador é responsável pela preservação, integridade e

confidencialidade dessas informações.

As informações são um recurso valioso para a operação das atividades da Guex. Por essa razão, tal como qualquer outro ativo da empresa, devem ser tratadas com diligência, ética e profissionalismo. Todos os colaboradores são responsáveis por proteger as informações, independentemente da forma de armazenamento ou transmissão.

Além disso, a Guex implementa um programa de segurança cibernética que inclui:

1. Identificação/avaliação de riscos (risk assessment) – A Guex realiza uma avaliação de riscos regular e abrangente para identificar os riscos internos e externos. Esta avaliação inclui a identificação de todos os ativos relevantes da Guex, sejam equipamentos, sistemas, processos ou dados, usados para seu correto funcionamento. Além disso, a Guex avalia as vulnerabilidades dos ativos em questão, identificando as possíveis ameaças e o grau de exposição dos ativos a elas. Vários cenários são considerados nessa avaliação, incluindo os possíveis impactos financeiros, operacionais e reputacionais, em caso de evento de segurança, assim como a expectativa de tal evento ocorrer.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, na avaliação inicial:

a) Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
b) Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso ("**Phishing**");
c) Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política; ou
d) Vazamento de informações durante tráfego de dados não criptografados.
e) Ações de prevenção e proteção – A Guex estabelece um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados na avaliação de riscos. Isso inclui o controle do acesso adequado aos ativos da Guex, a implementação de regras mínimas na definição de acesso a dispositivos corporativos, a disponibilização de autenticação de múltiplos fatores, a limitação do acesso a apenas recursos relevantes para o desempenho das atividades e a implementação de serviço de backup dos diversos ativos da Guex.

2. Monitoramento e Testes – A Guex implementa um programa de monitoramento e testes para detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico. Isso inclui a criação de mecanismos de monitoramento de todas as ações de proteção implementadas, a manutenção de inventários atualizados de hardware e software, a realização de testes de invasão externa e phishing, e a análise regular dos logs e as trilhas de auditoria criados.

O ambiente de TI da Guex será monitorado, por meio de indicadores e geração de históricos: (i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à

Internet e aos sistemas críticos da Guex; (iii) de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Guex; (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e (v) das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Para garantir as regras mencionadas nesta Política, a Guex deverá (a) Para os riscos associados a Phishing, conduzir treinamentos e campanhas periódicas, bem como testes de Phishing, (b) Realizar, a qualquer tempo, inspeção física nas máquinas de hardware;(c) Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; (d) Testar a vulnerabilidade e penetração do Website da Guex, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela Guex, ao menos anualmente.

3. Criação do plano de resposta – A Guex mantém um plano de resposta a incidentes de segurança cibernética, que inclui a comunicação interna e externa necessária em caso de incidente. Este plano é revisado e atualizado regularmente para garantir que permaneça eficaz e relevante para as necessidades da Guex. O plano de ação conta com mecanismos que asseguram a comunicação imediata para todos os colaboradores relevantes com relação a incidentes que possam gerar riscos à empresa, e prevê o acionamento dos colaboradores-chaves e contatos externos relevantes, inclusive de reguladores, considerando critérios e prazos vigentes, quando aplicável.

- Procedimento em caso de incidente - Uma vez que o Diretor de Compliance tenha sido acionado devido a um potencial incidente, este deverá atuar em conjunto com a área de TI para solução imediata do problema.

- Avaliação Inicial - Na etapa inicial, aspectos e decisões fundamentais deverão ser analisadas e tomadas após o incidente. Deverá ser realizada uma análise do que aconteceu, compreendendo motivos e consequências imediatas, bem como a gravidade da situação, devendo ser decidido a formalização ou não do incidente.

- Incidente Caracterizado - Se for caracterizado um incidente, devem ser tomar as medidas imediatas, que poderão abranger (i) se será registrado um boletim de ocorrência ou queixa crime, (ii) se há necessidade de informar à CVM ou mais alguma autoridade, (iii) se é necessário envolver consultor ou advogado externo; (iv) se haverá comunicação interna ou externa, em especial a Investidor que eventualmente tenha sido afetado; e (v) se houve prejuízo para a Guex, algum veículo de investimento ou investidor específico. Além disso, caso seja necessário, deverão ser definidos os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

- Recuperação - Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados, caso necessário. Será realizado um acompanhamento, com um sumário elaborado pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos

Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Guex, devem ser comunicados. Colaboradores externos relevantes deverão ser mantidos atualizados, caso seja necessário.

- Retomada - Por fim, essa fase é a de transição ao modo normal de operação e pode incluir a análise de projetos, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. Ademais, após eventual evento de contingência, o Diretor de Compliance deverá avaliar os prejuízos decorrentes da ocorrência e propor melhorias e investimentos para a redução dos riscos.

- Tratamento de Vazamento de Informações - Em caso de vazamento de informações confidenciais, reservadas ou privilegiadas, seja por ação involuntária ou não, a Guex iniciará imediatamente uma investigação interna para determinar a origem e o alcance do vazamento. Os colaboradores envolvidos serão notificados e receberão instruções específicas sobre como proceder. As partes afetadas serão informadas sobre o vazamento e a Guex tomará as medidas necessárias para mitigar os riscos associados, incluindo a notificação das autoridades competentes, quando aplicável. Todos os detalhes do incidente, incluindo as medidas tomadas em resposta, serão documentados e revisados para evitar recorrências futuras.

- Testes de Contingência - Os Testes de Contingência serão realizados com periodicidade mínima anual ou em virtude das mudanças ocorridas na Guex que assim o justifiquem, de modo a permitir que a Guex esteja sempre aprimorando sua infraestrutura para a continuação de suas atividades.

O objetivo do teste incluirá a avaliação se o Plano desenvolvido é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da Guex e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se o Plano pode ser ativado tempestivamente.

Os testes abrangerão os seguintes eventos, apenas de forma amostral, a saber:

- Testes dos nobreaks, verificando o status de funcionamento e do tempo de suporte das baterias com carga;
- Acesso aos sistemas e aos e-mails remotamente, de endereço externo;
- Acesso aos dados armazenados externamente; e
- Outros necessários à continuidade das atividades.
- O resultado de cada teste será registrado no documento de Teste de Contingência.

4. Governança – A Guex mantém o programa de segurança cibernética continuamente atualizado garantindo que ações, processos e indicadores sejam regularmente executados, retroalimentando a estratégia definida. O Comitê de Risco e Compliance tem como uma de suas funções tratar de segurança cibernética dentro da Guex, a revisão periódica do programa de segurança cibernética, a promoção e disseminação da cultura de segurança com a criação de canais de comunicação internos eficientes, e a definição e manutenção de indicadores de desempenho (key performance indicators).

Caso algum Colaborador identifique a conservação inadequada, utilização indevida de qualquer ativo (físico ou eletrônico) ou sistemas, deverá comunicar a ocorrência ao Diretor de Compliance.

O Diretor de Compliance será a responsável pela revisão da política cibernética e suas revisões, bem como para tratar e responder questões de segurança cibernética dentro da Guex.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Diretor de Compliance, devendo ser observado o procedimento previsto nesta Política em caso de vazamento de informação confidencial.

O Diretor de Compliance irá se consultar com setor de tecnologia de informação, tendo como objetivo a supervisão e monitoramento das regras de Segurança Cibernética, conforme aqui previsto.

Um plano de contingência e a continuidade dos sistemas e processos operacionais críticos deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação e segurança cibernética, incluindo a necessidade de planos de contingência, serão previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

A Guex exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

As informações podem existir em diversos formatos, incluindo sistemas de informação, diretórios de rede, bancos de dados, arquivos físicos, dispositivos eletrônicos, equipamentos portáteis e até mesmo por meio da comunicação oral. Se algum colaborador identificar a má conservação ou uso indevido de qualquer recurso (físico ou eletrônico) ou sistemas, ele deverá comunicar o incidente ao Diretor de Compliance.

Descrições e Características

Cada computador utilizado pelos colaboradores será fornecido com senhas individuais que permitem a identificação do usuário recente. O controle de acesso à informação centralizada é realizado pelo departamento de Compliance, que mantém o registro de contas e senhas. Os computadores, também, são configurados com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política, inclusive, mas não se limitando, a segregação das funções administrativas, operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Todos os arquivos armazenados nos servidores da Guex são protegidos por um backup diário,

firewall de última geração e sistema antivírus atualizado.

Os backups são realizados automaticamente todos os dias, utilizando ferramentas de armazenamento em nuvem da Microsoft. A Guex tem um sistema de backup e recuperação de arquivos que visa garantir a segurança das informações, a recuperação em caso de desastres e a integridade, confiabilidade e disponibilidade dos dados armazenados.

Todos os logs de sistemas são mantidos pela Guex por um período de 5 anos. A empresa verifica regularmente os padrões de todos os computadores, arquivos em rede, softwares, hardwares ou acessos não autorizados. Dessa forma, por meio dos logs, a Guex consegue garantir a integridade, autenticidade e capacidade de auditoria das informações e sistemas.

Todas as declarações de imprensa (envolvendo ou não a Guex) devem ser aprovadas previamente pelo Diretor de Compliance. Este poderá, a qualquer momento e sem aviso prévio, verificar o conteúdo das ligações telefônicas gravadas, os arquivos disponíveis no diretório interno e os e-mails enviados e recebidos.

O descarte de informações confidenciais armazenadas digitalmente deve ser realizado de maneira a impossibilitar sua recuperação. Documentos físicos contendo informações confidenciais que não precisam ser arquivados devem ser descartados imediatamente após seu uso, impedindo sua recuperação ou leitura.

Protocolo de Assinatura de Documentos de Confidencialidade por Colaboradores

Conforme estabelecido pelas diretrizes da Guex e em conformidade com as regulamentações aplicáveis, a Sociedade é obrigada a exigir que todos os seus colaboradores assinem, seja de forma manual ou eletrônica, um documento de confidencialidade. Esse documento deve abordar claramente as responsabilidades e obrigações dos profissionais em relação às informações confidenciais, reservadas ou privilegiadas que lhes foram confiadas em virtude do exercício de suas atividades profissionais. A única exceção a esta regra são as situações específicas permitidas por lei.

Este protocolo tem o objetivo de reforçar o compromisso dos profissionais com a confidencialidade, a integridade e a segurança das informações sob sua responsabilidade, e garantir que a Guex esteja em conformidade com todas as regulamentações pertinentes.

Em determinadas situações, para evitar a comunicação entre certos colaboradores ou departamentos, as áreas de Compliance e Tecnologia podem implementar barreiras de informação. Isso preserva a confidencialidade de certas informações confidenciais e impede sua comunicação entre diferentes áreas da Guex. Os colaboradores não devem compartilhar informações confidenciais sujeitas a barreiras de informação com outras áreas sem a aprovação prévia do Diretor de Compliance.

A Guex deverá proteger continuamente todos os ativos de informação da Guex contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso ou indesejado.

VII. PROCEDIMENTO DE TESTES PERIÓDICOS

O Diretor de Compliance deve realizar ou assegurar que sejam realizados testes de Compliance ao longo do ano fiscal. O objetivo desses testes é identificar e mitigar possíveis riscos aos quais a Guex possa estar exposta, e garantir a conformidade com as leis, regulamentações, políticas e procedimentos internos da Guex. Além disso, ele deve realizar um teste periódico específico de segurança para os sistemas de informações, especialmente os mantidos eletronicamente.

VIII. PROCEDIMENTO INTERNO DE REPORTE DE VIOLAÇÕES À CVM

O presente Manual dispõe sobre o procedimento interno de reporte de violações à CVM ("**Procedimento**"), que estabelece normas e procedimentos, a serem utilizados por todos os Colaboradores que tenham acesso a informações relevantes sobre a Guex com a finalidade de assegurar a comunicação à CVM de quaisquer violações às regulamentações emitidas por esta Autarquia.

Todos os Colaboradores deverão comunicar imediatamente ao Diretor de Compliance a identificação ou suspeita de quaisquer violações.

Em caso de violações relativas à legislação expedida pela CVM, ao Diretor de Compliance, deverá analisar o cadastro, as operações ou transações pertinentes. Após o prazo para regularização de eventuais situações de não conformidade, ou caso a suspeita se confirme após todas as análises, o Diretor deve apresentar um relatório sobre o caso.

IX. SEGREGAÇÃO DE ATIVIDADES

A Guex manterá a devida segregação entre as suas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

A segregação de atividades é um requisito essencial para que seja dado o efetivo cumprimento das atividades de consultoria de valores mobiliários.

O Diretor de Compliance possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos Diretores ou demais sócios da Guex.

A Área de Compliance atua de forma autônoma e independente, se reportando ao Diretor de Compliance.

A Guex adota um conjunto de procedimentos estabelecidos pelo Diretor de Compliance, com o objetivo de proibir e impedir o fluxo de informações privilegiadas e/ou sigilosas para outros departamentos, ou Colaboradores, da instituição que não estejam diretamente envolvidos na

atividade de consultoria de valores mobiliários.

A Guex realizará os melhores esforços para que a segregação das informações e suas atividades sejam sempre preservadas. Com o intuito de assegurar a completa segregação, os seguintes procedimentos operacionais serão adotados:

1. Instalação física com limitação de acesso de terceiros, serão adotadas medidas adicionais para garantir a devida segregação física das operações da Guex. Essas medidas incluem a delimitação de áreas para discussões confidenciais e a aplicação de políticas rígidas que proíbem tais discussões em espaços compartilhados;

2. A segregação informacional absoluta e inviolável da Guex e qualquer sociedade que os Colaboradores tenham relacionamento, os equipamentos devem ser utilizados apenas por aqueles autorizados e em circunstâncias específicas. Adicionalmente, a gestão e proteção das informações comuns serão reforçadas através do uso de tecnologia segura e práticas de gerenciamento de dados;

3. A preservação de informações confidenciais por todos os seus Colaboradores, proibindo a transferência de tais informações a pessoas não habilitadas ou que possam vir a utilizá-las indevidamente;

4. A implantação e manutenção de programa de treinamento de Colaboradores que tenham acesso a informações confidenciais e/ou participem de processo de consultoria de valores mobiliários. O programa incluirá orientações claras sobre as políticas de confidencialidade, expectativas de comportamento e as consequências para o não cumprimento dessas políticas. A participação de todos os Colaboradores relevantes será obrigatória e registrada para garantir a conformidade; e

5. O acesso restrito a arquivos, bem como à adoção de controles que restrinjam e permitam identificar as pessoas que tenham acesso às informações confidenciais.

Dessa forma, a Guex acredita que as medidas acima relacionadas são eficazes para cumprir os requisitos mínimos de segregação de atividades aplicados a sua realidade, buscando servir adequadamente seus clientes e cumprir com suas obrigações.

X. CONSIDERAÇÕES FINAIS

Este Manual não substitui a obrigação que cada Colaborador tem de usar o bom senso, discernimento e de, sempre que necessário, em caso de dúvidas, contatar o Diretor de Compliance diretamente ou através do e-mail compliance@guex.com.br

Quaisquer solicitações de exceções às regras descritas neste Manual devem ser encaminhadas ao Diretor de Compliance, que possui amplos poderes para aprovar exceções a este Manual, desde que a razão, natureza, prazo, e outras informações importantes sobre a decisão sejam devidamente formalizadas, sempre respeitando as leis e regulamentações aplicáveis.

Mediante a contratação/início do relacionamento profissional, e anualmente, todos os Colaboradores deverão aderir a este Manual através do preenchimento e assinatura do Formulário 'Conheça seu Colaborador' que será disponibilizado pelo Diretor de Compliance.

O Diretor de Compliance atualizará este Manual dentro de um período de tempo razoável depois que ocorrerem mudanças nas leis e normas aplicáveis, ou sempre que considerar apropriado e, subsequentemente, divulgará a todos os Colaboradores e no website da Guex: www.guex.com.br

* * * * *