MANUAL DE *COMPLIANCE* E CONTROLES INTERNOS

Versão:	Motivo da alteração:	Data:	Aprovado por:	Data da aprovação:
03	Terceira versão	Janeiro/2025	Manuela Aguiar	13/01/2025

1. INTRODUÇÃO

1.1. Este Manual de *Compliance* e Controles Internos ("Manual") foi desenvolvido pelo departamento de *compliance* com o objetivo de estabelecer regras, procedimentos, bem como descrever os controles internos que orientam os sócios, administradores, empregados, estagiários, diretores e demais colaboradores ("Colaborador" ou "Colaboradores") da HCO Group S.A. ("HCO") perante suas atividades.

1.2. As regras e procedimentos aqui previstos visam garantir o atendimento às normas, políticas e regulamentações vigentes, referentes às diversas modalidades de investimento, à própria atividade de gestão e aos padrões éticos e profissionais.

1.3. Dessa forma, objetivam reduzir a frequência de surgimento de eventos, facilitar a identificação de eventos e mitigar riscos decorrentes de eventos quando estes surgirem, bem como, disseminar a cultura de controles para garantir o cumprimento das normas contidas na Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM nº 21"), no Código de Administração e Gestão de Recursos de Terceiros da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA, conforme alterado periodicamente, e nas demais normas estabelecidas pelos órgãos reguladores e autorreguladores.

1.4. O presente Manual foi elaborado e deve ser interpretado em consonância com os demais manuais e políticas da HCO, e deve ser revisado e atualizado anualmente, conforme necessário, pelo departamento de *compliance*, com o apoio das áreas administrativa e de tecnologia, a fim de incorporar medidas relacionadas às atividades e riscos novos ou anteriormente não abordados.

2. ABRANGÊNCIA

Este Manual aplica-se a todos os Colaboradores da HCO.

3. PRINCÍPIOS NORTEADORES

3.1. As atividades de controle devem ser constantemente avaliadas, tomando como referência as boas práticas de governança corporativa.

3.2. Controles internos consistem em um ou mais processos desenvolvidos para garantir o atingimento dos objetivos da HCO, com relação a:

I. eficiência e efetividade operacional;

II. confiança nos registros de dados e informações;

III. conformidade; e

IV. abordagem baseada em gestão de risco.

4. DIRETRIZES

4.1. Este Manual tem como diretrizes:

I. disseminar a cultura sobre a importância dos controles internos a todos os Colaboradores;

II. assegurar o cumprimento das normas e regulamentos e aderência às políticas e procedimentos internos;

III. alinhar a estrutura dos controles internos aos objetivos do negócio e aos riscos dele decorrentes;

IV. criar o arcabouço necessário para a existência de atribuição de responsabilidades e delegação de autoridade, observada a estrutura hierárquica da HCO;

V. possibilitar a elaboração de relatórios sobre a situação dos controles internos;

VI. estabelecer os fluxos de aprovação mediante alçadas; e

VII. assegurar a revisão periódica dos processos de controles internos.

5. RESPONSABILIDADES

5.1. Implementação e Manutenção de Processos de Controles Internos: os gestores de cada uma das áreas da HCO são responsáveis por estabelecer, manter, promover e avaliar as atividades desempenhadas e estabelecer controles internos adequados e eficazes, bem como documentá-los de maneira clara e objetiva.

5.2. O departamento de *compliance* deverá receber de cada um dos gestores o *status* dos controles internos por eles implantados, incluindo os eventos negativos e impactos. De posse dos relatórios, o Diretor de *Compliance* e Risco emitirá um relatório com eventuais propostas para a Diretoria.

5.3. Análise dos Processos de Controles Internos: o Diretor de *Compliance* e Risco é o encarregado pela definição dos métodos de avaliação e monitoramento dos processos de controles internos da HCO, sendo também responsável pelo atendimento aos órgãos reguladores e autorreguladores.

5.4. Avaliação dos Processos de Controles Internos: o Diretor de *Compliance* e Risco é responsável por promover a avaliação independente das atividades desenvolvidas pelas diversas áreas da HCO, de modo a aferir a adequação dos controles estabelecidos ao cumprimento das normas e regulamentos.

5.5. O processo de aferição é realizado através de exames de aderência nos processos existentes e documentados.

5.6. A periodicidade e os exames de aderência a serem realizados são definidos pelo Diretor de *Compliance* e Risco, de acordo com os eventos reportados, sempre respeitando os prazos estabelecidos pelas normas e regulamentos.

5.7. Acompanhamento dos Processos de Controles Internos: o Diretor de *Compliance* e Risco é responsável por acompanhar o resultado dos testes de aderência e supervisionar as atividades de controles internos da HCO.

5.8. Adicionalmente, o Diretor de *Compliance* e Risco monitorará a qualidade e integridade dos mecanismos de controles internos da HCO, apresentando as recomendações de aprimoramento de manuais, políticas, códigos, práticas e procedimentos que entender necessárias.

5.9. O Diretor de *Compliance* e Risco também tem acesso regular à capacitação e treinamento dos Colaboradores ou futuros Colaboradores, podendo alterar os critérios, medidas e manuais, políticas e códigos, conforme seu discernimento.

5.10. Anualmente, e de acordo com o artigo 25 da Resolução CVM nº 21, a HCO emitirá um relatório acerca dos controles internos com a conclusão dos exames efetuados, que ficará disponível para a CVM na sede da HCO.

5.11. Convém ressaltar que a HCO também dispõe de um Comitê de *Compliance* e Gestão com atribuição para deliberar sobre matérias e diretrizes de *Compliance* da HCO e de seus Colaboradores.

6. CONFLITO DE INTERESSE

6.1. De forma a evitar possíveis conflitos de interesse, uma vez constatada a incidência ou a possibilidade de qualquer conflito, o Diretor de *Compliance* e Risco terá comunicação direta com os administradores e sócios da HCO para realizar relato dos resultados decorrentes das atividades relacionadas à suas funções, incluindo possíveis irregularidades ou falhas identificadas.

6.2. Buscando conceder ainda maior transparência a todos os seus *stakeholders*, a HCO informa que a Huma Capital Ltda., inscrita no CNPJ sob o nº 49.494.976/0001-57 ("Huma Capital") exerce influência significativa sobre a HCO, nos termos do artigo 243, §§ 4º e 5º, da Lei nº 6.404, de 15 de dezembro de 1976, conforme alterada ("Lei das S.A."). Desta forma, ambas as sociedades são consideradas coligadas, conforme conceito estabelecido pelo artigo 243, § 1º, da Lei das S.A.

6.3. À luz do exposto no item 6.2 acima, entendemos que não há a configuração de conflitos de interesse nas atuações do (i) Sr. Ariel Araujo de Almeida, na posição de Diretor de Gestão, da (ii) Sra. Manuela de Siqueira Aguiar Précaro, na posição de Diretora de *Compliance* e Risco, e do (iii) Sr. Tadeu Ferreira Jorge, na posição de Diretor sem designação específica, enquanto executivos tanto da Huma Capital quanto da HCO, diante da faculdade prevista pelos artigos 4º, § 4º, e 26, § 5º, inc. III, ambos da Resolução CVM nº 21. Entretanto, caso seja identificada uma situação que tenha o potencial de se configurar como um conflito de interesses entre a Huma Capital e a HCO, a HCO, os fundos sob sua gestão e/ou seus investidores, a HCO notificará seus investidores sobre tal situação e tomará todas as medidas para que seja convocada uma assembleia geral de cotistas do respectivo fundo de investimento para que tal situação seja discutida e deliberada.

7. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

7.1. Esta política tem como objetivos:

I. permitir que a HCO atenda à regulamentação, legislação e autorregulação aplicáveis;

II. manter o nível de segurança da organização em um patamar definido como adequado pela HCO; e

III. garantir que as diretrizes contidas nesta política sejam praticadas, por meio da implementação de controles que visam garantir a confidencialidade, a integridade e a disponibilidade das informações.

7.2. Para atingir este objetivo, a HCO estabelece a presente política como um dos pilares de sua estratégia de segurança, a qual deve ser seguida e implementada para garantir que os ativos sejam protegidos de acordo com a sua importância estratégica para a organização.

7.3. A política ora tratada define-se como um documento que expressa a posição da organização sobre a segurança, quais são seus valores e direcionamentos para minimizar os riscos sobre seus ativos. Desta forma, ela estabelece a linha mestra de atuação da HCO em relação a todos os aspectos da segurança da informação, incluindo equipamentos, bens, informações e pessoas.

7.4. A presente política tem como princípios assegurar a:

I. Identificação: garantir que qualquer indivíduo seja identificado inequivocamente;

II. Autenticação: garantir que a identidade de cada pessoa ou recurso seja expressamente comprovada;

III. Autorização: garantir que somente as pessoas e recursos permitidos tenham acesso aos ativos;

IV. Confidencialidade: garantir que as informações sejam acessadas apenas por aqueles expressamente autorizados;

V. Integridade: preservar a integridade das informações, salvaguardando-as contra ações não autorizadas e garantindo que todas as informações estejam exatas e completas durante a sua criação, uso, guarda e destruição; e

VI. Disponibilidade: garantir que os usuários, quando devidamente autorizados, tenham acesso às informações e instalações sempre que necessitarem.

7.5. Com a finalidade de assegurar que os princípios acima sejam observados, a HCO desenvolve as seguintes atividades:

I. classificação da informação:

A. controle de acesso às informações; e

B. rastreamento e monitoramento;

II. avaliação de risco:

A. controle de mudanças;

B. plano de contingência; e

C. segurança física dos dispositivos onde é armazenada e por onde transita a informação;

III. testes de segurança e de continuidade dos negócios.

7.6. Este documento serve como um guia de melhores práticas em relação à segurança da informação e tem o propósito de oferecer uma base comum de atuação para ser usado por aqueles que são responsáveis pela criação, implementação e manutenção de processos, procedimentos, sistemas, tecnologias, conhecimento, estratégias, serviços, campanhas e quaisquer outros ativos que compõem o dia a dia da HCO. A empresa tem como compromisso assegurar que as orientações definidas sejam seguidas por toda a organização.

7.8. Esta Política se aplica aos Colaboradores e ativos descritos abaixo:

I. **Colaboradores**: todas as pessoas que, de alguma forma, prestem serviços para a HCO, sejam elas diretores, sócios, empregados, estagiários ou terceiros contratados. Todos devem dar cumprimento às regras definidas nesta política; e

II. **Ativos**: todo equipamento, instalação, sistema e informação, bem como quaisquer outros bens, tangíveis ou intangíveis, de propriedade ou geridos pela HCO. Da mesma forma, se aplica a todas as plataformas de *hardware* e a todos os sistemas operacionais e aplicativos utilizados. Aplica-se também a qualquer meio onde a informação possa ser armazenada, incluindo mídias magnéticas, discos ópticos, "nuvens" de armazenamento, informações impressas em papel e material de *marketing*.

7.7. Antes de efetuar ações que envolvam acesso, uso, alteração, armazenamento, transmissão, destruição ou qualquer outra atividade envolvendo ativos da empresa, o usuário deve consultar esta Política para certificar-se de que a atividade é permitida. Toda e qualquer atividade que não seja claramente permitida é proibida. Em caso de dúvida o usuário deve consultar o departamento de *compliance* e o responsável pela tecnologia para assegurar-se que a atividade é permitida. Cabe ao responsável pelo departamento de *compliance* e o responsável pela tecnologia avaliar os riscos das atividades não previstas nas diretrizes de segurança da empresa, levando ao conhecimento do Comitê de *Compliance* e Gestão competente a prática dessas atividades.

8. PRIVACIDADE

8.1. Todos os ativos pertencem à HCO e, portanto, a HCO tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos de rede ou ''nuvem'', os quais se encontrem fisicamente no mobiliário da empresa, como, por exemplo, em mesas, estantes, gaveteiros, armários etc. Dessa forma, ainda que o Colaborador possa utilizar-se da estrutura da empresa para algum uso particular não conflitante, tais informações podem ser acessadas pela HCO mesmo sem o prévio consentimento do respectivo Colaborador.

8.2. Com relação a qualquer troca de informações por meio dos ativos da HCO, incluindo, mas não se limitando, a *e-mails*, mensagens instantâneas e às ligações telefônicas, a HCO se reserva ao direito de monitorar tais informações e seus conteúdos, gravar registros das ligações e das respectivas conversas, bem como consultá-las sem prévio aviso ao Colaborador.

8.3. Sem prejuízo do acima exposto, a HCO garante que toda escuta a conversas telefônicas e consulta a dados depende do prévio consentimento do departamento de *compliance*.

9. SEGURANÇA DA INFORMAÇÃO CONFIDENCIAL

9.1. A HCO mantém um inventário atualizado que identifica e documenta a existência e as principais características de todos os ativos de informação, como base de dados, arquivos, planos de continuidade, entre outros. Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da HCO, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

9.2. Em caso de determinado Colaborador passar a exercer atividade ligada a outra área da HCO, tal Colaborador terá acesso apenas às informações relativas a esta área, das quais necessite para o exercício da nova atividade, deixando de ter permissão de acesso aos dados, arquivos, documentos e demais informações restritas à atividade exercida anteriormente. Em caso de desligamento da HCO, o Colaborador deixará imediatamente de ter acesso a qualquer ativo de informação interna.

9.3. Qualquer informação sobre a HCO, ou de qualquer natureza relativa às suas atividades, aos seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na HCO, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado previamente e por escrito pelo Diretor de *Compliance* e Risco.

9.4. É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos à HCO com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

9.5. A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da HCO e de seus clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

9.6. Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da HCO.

9.7. O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

9.8. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de forma a impossibilitar sua recuperação, por meio por exemplo, mas não se limitando, de uma trituradora.

9.9. Adicionalmente, os Colaboradores devem se abster de utilizar *hard drives*, *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na HCO.

9.10. É proibida a conexão de equipamentos na rede da HCO que não estejam previamente autorizados pelo sócio gestor responsável.

9.11. Cada Colaborador é responsável por manter o controle da segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

9.12. O envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de *e-mails* com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da HCO.

9.13. Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome da HCO, ou utilizar material, marca e logotipos da HCO para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

9.14. O Diretor de *Compliance* e Risco também monitorará e será avisado por *e-mail* em caso de tentativa de acesso aos diretórios e *logins* virtuais no servidor protegidos por senha. O Diretor de *Compliance* e Risco elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

9.15. Programas instalados nos computadores, principalmente via *internet* (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na HCO. Não é permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos *softwares* dos Colaboradores para aspectos profissionais e pessoais.

9.16. Todas as informações do servidor da HCO, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor interno. Nesse servidor, as informações são segregadas por área, sendo armazenadas via *backup*.

9.17. A rotina de *backup* contempla o método abaixo descrito, garantindo a salvaguarda de todos os dados, sendo eles banco de dados, documentos, planilhas e diversos outros guardados na área de armazenamento.

9.18. Método: *backup online* executado diariamente. Esse *backup* copia tudo o que é modificado ou criado, possui fácil recuperação e visualização das informações copiadas.

9.19. Em caso de divulgação indevida de qualquer informação confidencial, o Diretor de *Compliance* e Risco apurará o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador. Serão realizados testes de segurança para os sistemas de informações utilizados pela HCO, em periodicidade, no mínimo, anual, para garantir a efetividade dos controles internos mencionados neste Manual, especialmente as informações mantidas em meio eletrônico.

10. DEVERES E RESPONSABILIDADES

10.1. São deveres de todos os Colaboradores no âmbito desta política:

I. preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

II. cumprir a presente política, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

III. utilizar os sistemas de informações e os recursos relacionados somente para os fins previstos pela área de tecnologia;

IV. cumprir as regras específicas de proteção estabelecidas aos ativos de informação;

V. manter o caráter sigiloso da senha de acesso aos recursos e sistemas;

VI. não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;

VII. responder por todo e qualquer acesso aos recursos da empresa, bem como pelos efeitos decorrentes de acesso efetivado através de seu código de identificação, ou outro atributo para esse fim utilizado;

VIII. solicitar acesso às informações restritas somente quando houver real necessidade de acessar o recurso;

IX. respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, sob pena de violação da legislação de propriedade intelectual pertinente; e

X. comunicar ao seu superior imediato e ao departamento de *compliance* quando do conhecimento de qualquer irregularidade ou desvio verificado no âmbito da presente política.

11. RESPONSABILIDADES GERAIS

11.1. Cada área que detém ativos de processamento e de informação é responsável por estes.

11.2. Cada gestor de área deve fornecer à estrutura responsável pela tecnologia, informações tempestivas sobre movimentação de funcionários de sua equipe (desligamento, contratação, transferência etc.) para que os responsáveis promovam a criação, modificação ou cancelamento da respectiva permissão de acesso.

12. RESPONSABILIDADES DO DEPARTAMENTO DE TECNOLOGIA

I. estabelecer as regras de proteção dos ativos da HCO;

II. revisar frequentemente as regras de proteção estabelecidas;

III. restringir e controlar o acesso e privilégios de usuários remotos e externos;

IV. auxiliar os departamentos administrativo e de *compliance* a elaborar e a manter atualizado o Plano de Contingência e Continuidade dos Negócios;

V. executar as regras de proteção estabelecidas por esta política;

VI. detectar, identificar, registrar e comunicar à chefia violações ou tentativas de acesso não autorizadas;

VII. definir e aplicar, para cada usuário, restrições de acesso à rede, como horários e dias autorizados, dentre outras;

VIII. limitar ao período da contratação o prazo de validade das contas de prestadores de serviço;

IX. solicitar e gerir, quando necessário, auditoria para verificação de acessos indevidos;

X. solicitar, quando julgar necessário, o bloqueio de chaves de acesso de usuários;

XI. excluir ou desabilitar as contas inativas;

XII. fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;

XIII. garantir o cumprimento do procedimento de *backup* para os servidores e ativos; e

XIV. organizar treinamentos relacionados à segurança dos ativos de informação sempre que necessário.

13. RESPONSABILIDADES DO DEPARTAMENTO DE *COMPLIANCE*

I. assessorar a HCO na elaboração e verificação da legalidade dos regulamentos, termos, políticas e controles utilizados para proteger os ativos de informação;

II. liderar o processo de apuração das responsabilidades e causas quando da ocorrência de incidentes ou violações de segurança da informação aos regulamentos internos e externos da HCO, ainda que auxiliado pela área de tecnologia;

III. assegurar que as atividades da HCO sejam desenvolvidas com base nos princípios estabelecidos em seus manuais/políticas internos e em consonância com a regulamentação, legislação e autorregulação aplicáveis;

IV. dirimir ou ao menos mitigar a existência de conflitos de interesse relacionados ao desenvolvimento das atividades da HCO, especialmente para fins do disposto nesta política;

V. elaborar e controlar a política de Uso dos Recursos de Informática da HCO, prevista no item 15 deste Manual, inclusive quanto ao acesso de USB e CD-ROM, criando os perfis de acesso e designando-os a cada Colaborador de acordo com as atividades por ele desenvolvidas e com o cargo por ele ocupado;

VI. atualizar a política de Uso dos Recursos de Informática, bem como solicitar à área de tecnologia a liberação ou o bloqueio de perfis de acordo com as necessidades verificadas ou sob demanda dos Colaboradores quando julgar pertinente; e

VII. aprovar a criação ou exclusão de usuários quando houver contratação ou demissão de efetivos ou de estagiários, sendo certo que os usuários novos devem ser cadastrados sem nenhum acesso, os quais devem ser solicitados posteriormente pela sua gerência.

13.1. Para permitir que cumpra suas obrigações conforme acima expostas, o departamento de *compliance* possui acesso irrestrito a todas as dependências da HCO, inclusive salas com controle de acesso, bem como a toda a rede interna.

14. RESPONSABILIDADE DO DEPARTAMENTO JURÍDICO

I. assessorar a HCO na elaboração e verificação da legalidade dos regulamentos, termos, políticas e controles utilizados para proteger os ativos de informação;

II. garantir que os contratos celebrados com terceiros, sempre que necessário, contenham cláusula que preserve a segurança das informações da HCO; e

III. garantir que a existência das diretrizes estabelecidas com base nesta política e a necessidade do cumprimento de suas premissas sejam referenciadas nos contratos e acordos com terceiros, bem como nos contratos firmados com os Colaboradores da HCO, de forma que cada um saiba suas obrigações, direitos e deveres no âmbito desta política.

15. USO DOS RECURSOS DE INFORMÁTICA

Uso do E-mail:

I. uso do *e-mail* na HCO está baseado nas premissas de civilidade, eficiência e rapidez, sempre objetivando aumentar a produtividade nos trabalhos diários. Com isso em vista, seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização desta ferramenta;

II. o usuário é o único responsável pelo conteúdo das transmissões feitas através do *e-mail* a partir de sua senha ou conta;

III. as mensagens de *e-mail* são confidenciais, somente podendo ser acessadas pelo remetente e seu(s) destinatário(s). É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela, com exceção do quanto disposto no item 8.1. deste Manual;

IV. não devem ser abertos arquivos ou executados programas anexados aos *e-mails* que sejam suspeitos ou não conhecidos sem antes verificá-los com um antivírus ou sem a prévia verificação do responsável pela tecnologia;

V. devem estar desligadas as opções que permitam abrir ou executar automaticamente arquivos ou programas anexados às mensagens;

VI. não deve ser utilizado *e-mail* para fins ilegais;

VII. não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através deste serviço;

VIII. não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas sem limitação, direitos de propriedade intelectual;

IX. não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis;

X. o Colaborador não pode obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço;

XI. não devem ser utilizados os serviços de *e-mail* para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Tróia" ou outro programa prejudicial;

XII. não devem ser transmitidas mensagens não solicitadas, conhecidas como *spam* ou *junk mail*, correntes, *chain letters* ou distribuição em massa de mensagens não solicitadas;

XIII. mensagens com assuntos confidenciais não devem ser impressas em impressoras usadas por outros usuários, sem que você esteja cuidando para retirar a impressão antes do acesso físico ao conteúdo impresso, de forma inadvertida, pelos demais usuários;

XIV. o *e-mail* deve estar ativo sempre que o usuário estiver trabalhando no microcomputador. Quando este se afastar de sua estação de trabalho, deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal;

XV. é proibido aos administradores de rede ou *e-mail* ler mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte; e

XVI. não é permitido enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

Uso do Telefone:

I. o uso de telefone localizado fora das dependências da HCO para discussão de assuntos confidenciais internos pode ser necessário, porém pode gerar exposição de segurança, portanto, certifique-se de que não está sendo escutado por pessoas próximas;

II. não deixe mensagens confidenciais em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas; e

III. quando estiver coordenando uma teleconferência, certifique-se de que todos os participantes foram devidamente autorizados antes de começar a reunião.

Uso da Internet:

I. Alguns *sites* (páginas da *internet*) contêm ou distribuem material não apropriado ao ambiente de trabalho, portanto, os Colaboradores não devem acessar tais *sites*, tampouco distribuir/obter material similar enquanto nas premissas da HCO;

II. os acessos a *sites* podem estar sendo monitorados a qualquer tempo, portanto, em caso de dúvida, verifique junto ao seu gestor ou a área de tecnologia se o respectivo *site* pode ser acessado pelos Colaboradores;

III. não é permitido o uso de serviços de mensagens ou *chat* para uso pessoal (Whatsapp, AIM, Messenger etc.);

IV. os serviços de mensagens fornecidos pela HCO apenas devem ser utilizados para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas na empresa;

V. não é permitido o acesso das estações de trabalho a *webmail* (Hotmail, Gmail, Bol, Yahoo, UOL, AOL etc.);

VI. não é permitido o uso de compartilhadores de informações como redes Peer-to-Peer, também conhecidas como redes P2P (Kazaa, eDonkey, eMule, BitTorrent etc.) dentro das dependências da HCO; e

VII. não é permitido o *download* de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

Uso das Impressoras:

I. quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;

II. esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;

III. a impressora apenas deve ser utilizada para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pela HCO; e

IV. impressões coloridas devem ser feitas apenas em caráter excepcional, quando a utilização da cor interferir na compreensão do documento ou quando a situação assim exigir.

Senhas:

15.1. A senha é o meio de validação de acessos a recursos e serviços, funcionando como a assinatura digital do Colaborador, portanto, devem ser verificados os seguintes cuidados básicos para sua proteção:

I. manter sua confidencialidade; e

II. criar senhas fortes, respeitando, ao menos, os critérios abaixo:

A. as senhas não podem ser óbvias, como senhas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex.: nome ou data de nascimento do usuário); e

B. devem ter pelo menos 6 (seis) caracteres.

Proteção do Patrimônio:

15.2. Integram o patrimônio físico e intelectual da empresa, seus imóveis, instalações, veículos, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados que devem ser protegidos pelos funcionários, não podendo estes serem utilizados para obtenção de vantagens pessoais e nem fornecidos à terceiros, independentemente do fim.

15.3. Não podem ser utilizados equipamentos ou outros recursos da HCO para fins particulares, salvo se previamente autorizados pelo superior hierárquico imediato, sendo referida aprovação vetada nos casos em que esta:

I. interferir no seu trabalho;

III. interferir ou concorrer com os negócios da HCO;

IV. fornecer informação a terceiros;

V. envolver solicitação comercial ou outra solicitação não apropriada ao negócio; e

VI. envolver custo adicional para a HCO.

16. PROTEÇÃO AO PATRIMÔNIO ELETRÔNICO

16.1. O vírus de computador é um programa desenhado para causar perda ou alteração de dados do computador, com isso em vista, todo equipamento da HCO deve ter um programa antivírus instalado.

16.2. Os softwares antivírus devem ser atualizados diariamente e de forma automática.

16.3. O Colaborador, ao receber algum e-mail alertando sobre vírus, não deve encaminhá-lo a outras pessoas, pois geralmente estes alertas são falsos. De toda forma, permanecendo a dúvida, o Colaborador deve entrar em contato com a área de tecnologia para maiores explicações e suporte técnico.

Vulnerabilidades:

16.4. O sistema operacional deve sempre estar atualizado, para isso, ele deve estar configurado para atualização automática.

Aquisição de Software e Direitos Autorais:

16.5. A maioria das informações e *softwares* que estão disponíveis em domínio público (incluindo a *internet*) estão protegidos por leis de propriedade intelectual, portanto:

I. não é permitido obter *softwares*, imagens etc. (*download*) destas fontes para uso na empresa, exceto quando houver permissão explícita por parte do respectivo proprietário e autorização por parte da HCO ou quando a informação for inequivocamente de utilização pública;

II. deve-se ler e compreender todas as restrições dos direitos autorais do *software* e, caso a HCO não possa cumprir com as condições estipuladas, não é permitido realizar o *download*, bem como utilizar o respectivo material;

III. o Colaborador deve garantir que cumpre com os requerimentos ou limitações do *software* (ex.: não pode ser utilizado para fins comerciais, não cobrar de outros o uso do *software* etc.) antes de realizar o respectivo *download*; e

IV. em caso de dúvidas em relação às licenças ou a qualquer dos pontos acima, o Colaborador deve entrar em contato com o departamento de *compliance*.

Backup e Restauração de Sistemas:

16.6. A importância dos *backups* na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

16.7. Cada departamento/usuário tem acesso a pelo menos uma pasta no servidor de arquivos. Todos os documentos relacionados ao negócio devem ser copiados nestas pastas.

16.8. O *backup* dos servidores é executado pela equipe de tecnologia responsável por estes.

16.9. Os *backups* são realizados todos os dias com retenção em disco por 1 (uma) semana. No último domingo de cada mês, duas cópias completas de todos os arquivos são realizadas e armazenadas, a primeira em uma área reservada dentro das dependências da HCO e a segunda em mídia localizada fora das referidas dependências.

17. MESA LIMPA

17.1. A política de mesa limpa consiste em não deixar informações confidenciais ou bens da HCO, incluindo, mas não se limitando a papéis, *pen-drives*, CDs ou quaisquer outros tipos de mídias removíveis, acessíveis a outras pessoas sem a devida proteção, quando o funcionário estiver fora de sua estação de trabalho.

Tela Limpa:

17.2. Computadores, *notebooks* e *handhelds* devem estar protegidos por senha quando não estiverem sendo assistidos.

17.3. Todos os computadores devem ter proteção de tela automática com senha habilitada para acionamento no tempo máximo de 5 (cinco) minutos de inativação.

Notificações de incidentes de segurança:

17.4. Qualquer suspeita de ocorrência de incidente de segurança deve ser informada à área de tecnologia. Nenhum Colaborador deve investigar por conta própria ou tomar ações para se defender de eventual ataque, a não ser que seja instruído desta forma pela área de tecnologia. A área de tecnologia está capacitada para conter as exposições, analisar os impactos à HCO e conduzir investigações, coletando evidências para possíveis ações jurídicas.

18. POLÍTICA DE SIGILO DA INFORMAÇÃO

18.1. Esta política tem os seguintes objetivos:

I. expor as normas e procedimentos de proteção do sigilo das informações, em cumprimento das determinações legais aplicáveis, em especial às normas que tratam do sigilo bancário;

II. evitar a divulgação de dados e informações sobre as operações passivas (relacionamento com clientes) e ativas (operações com ativos sob gestão) da HCO, de forma a mantê-las sob sigilo; e

III. determinar as condições em que dados e informações sobre as operações passivas (relacionamento com clientes) e ativas (operações com ativos sob gestão) da HCO podem ser reveladas a terceiros.

18.2. A aplicação e monitoramento da presente política cabe ao departamento de *compliance*, obedecidas as especificações adiante elencadas:

I. os Colaboradores devem proteger a confidencialidade de quaisquer informações obtidas durante o exercício de suas funções na HCO, que não devem ser divulgadas a terceiros e/ou divulgadas ou disponibilizadas em domínio público;

II. a obrigação de sigilo prevista no item I (um), anterior, se aplica mesmo após a rescisão do vínculo do Colaborador da HCO, qualquer que seja a razão, permanecendo o Colaborador obrigado a manter sigilo e a proteger a confidencialidade das informações obtidas durante o exercício de suas funções na HCO; e

III. são informações confidenciais da HCO ("Informações Confidenciais"), as quais não devem ser disponibilizadas em domínio público ou a terceiros:

A. operações, estratégias, resultados, ativos, dados e projeções referentes às operações ativas e passivas da HCO, em especial aqueles que possam levar a uma vantagem competitiva da HCO frente a seus concorrentes;

B. informações sobre os planos de negócios da HCO;

C. Informações Confidenciais sobre Colaboradores da HCO; e

D. informações sobre clientes, distribuidores e fornecedores da HCO.

18.3. As informações relativas às atividades da HCO ou às suas controladoras, incluindo, mas não se limitando a textos, projetos, análises, informações relativas a clientes, Colaboradores, prestadores de serviços, parceiros comerciais, dados de cotistas

e operações financeiras, inclusive dados pessoais dos envolvidos, informações de emissores de títulos e valores mobiliários, estruturas de operações de financiamentos, incluindo seus envolvidos, segredos de mercado, *know-how*, melhorias, programas de treinamento, manuais ou materiais, informações técnicas, fontes codificadas de linguagem de computador, contratos, procedimentos, listas de mala direta, listas de preços, dados financeiros ou de outra natureza, planos de negócios, livros de códigos, faturas ou quaisquer outros relatórios financeiros, programas de computador, sistemas de *software*, base de dados, discos e impressos, planos (comercial, técnico ou qualquer outro), correspondências, relatórios internos, arquivos pessoais, material de vendas e propaganda, estratégia de *marketing*, números de telefone, nomes, endereços, estudos, compilações, previsões, informações técnicas, financeiras ou comerciais, informações pessoais de terceiros ou quaisquer outras informações, escritas ou não.

18.4. Questões envolvendo Informações Confidenciais de titularidade da HCO não devem ser discutidas pelos Colaboradores em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes etc.

18.5. Os *e-mails* disponibilizados pela HCO às pessoas autorizadas devem ser utilizados exclusivamente para mensagens de âmbito profissional e não podem, em hipótese alguma, ser usados para transmitir ou retransmitir mensagens ou seus anexos de qualquer natureza e conteúdo.

18.6. Os Colaboradores ficam expressamente vedados de utilizar quaisquer informações de terceiros ou de efetuar a transmissão de informações a terceiros que possam ser qualificadas como *insider trading* ou como *front running*.

18.7. Os Colaboradores respondem individualmente, civil e criminalmente, pela divulgação indevida de Informações Confidenciais ou pela divulgação de quaisquer informações que tenham por objetivo atingir a honra ou a imagem da HCO ou dissuadir seu relacionamento com clientes.

18.8. As Informações Confidenciais de clientes enviadas ou entregues à HCO para execução de transações são protegidas por lei. O compartilhamento destas Informações Confidenciais com terceiros depende de expressa autorização dos clientes, por escrito.

18.9. Na hipótese de vazamento de Informações Confidenciais, reservadas ou privilegiadas, ainda que decorrentes de ações involuntárias, deverá ser informado ao Diretor de Compliance, Risco e PLD imediatamente. O Diretor de Compliance, Risco e

PLD determinará quais membros da administração da HCO e, se aplicável, agências reguladoras e de segurança pública, deverão ser notificados. O Diretor de Compliance, Risco e PLD, avaliará os seguintes critérios: (i) identificação de quais informações foram divulgadas; (ii) avaliação do tipo de incidente ocorrido; (iii) avaliação de necessidade de notificação das partes internas e externas apropriadas; (iv) avaliação da necessidade de publicação de fato ao mercado, nos termos da regulamentação aplicável; e (v) determinação do responsável que arcará com as perdas decorrentes do incidente, com base no processo de investigação a ser instaurado, com o objetivo de identificar as causas do vazamento, a responsabilidade dos envolvidos e as medidas corretivas necessárias, além de sanções cabíveis, conforme disposto na cláusula 18.7 deste Manual. De qualquer forma, partes afetadas por eventual vazamento de Informações Confidenciais serão devidamente notificadas, bem como os órgãos competentes, conforme aplicável, serão informados do incidente, visando à mitigação dos danos potenciais. Portanto, a HCO se compromete a adotar todas as medidas administrativas, técnicas e organizacionais necessárias para prevenir novos incidentes e assegurar a proteção contínua de todas as Informações Confidenciais, em observância às normas de proteção de dados.

19. PLANO DE CONTINUIDADE DOS NEGÓCIOS

19.1. A HCO, em atendimento à regulamentação em vigor e às boas práticas no desenvolvimento da atividade de administração de carteiras, formulou o presente Plano de Continuidade dos Negócios ("Plano"), que tem por objetivo nortear a forma de identificar, prevenir e atuar em momentos de contingência, definindo as áreas prioritárias e procedimentos para garantir a continuidade do negócio.

19.2. O departamento de *compliance* deve se certificar da implementação do Plano para garantir a continuidade dos processos críticos da instituição em casos de eventos inesperados que afetem parte ou a totalidade da capacidade operacional da HCO, assegurando a realização de testes periódicos que atestem sua efetividade.

19.3. Dentre os principais eventos a serem considerados, podem ser verificados os seguintes:

I. incêndio;

II. alagamento;

III. sabotagem;

IV. terrorismo/pirataria;

V. furacão;

VI. desordem civil;

VII. roubo;

VIII. falta de energia; e

IX. falha aleatória de sistema crítico para a HCO.

Modelo de Atividade, Infraestrutura e Necessidades do Negócio:

19.4. A HCO é uma instituição não financeira focada na atividade de administração de carteiras de valores mobiliários, modalidade de gestor de recursos.

Infraestrutura Física e Tecnológica (Continuidade das Atividades Realizadas Cotidianamente):

19.5. As necessidades da HCO em termos de recursos físicos e tecnológicos tendem a crescer com o desenvolvimento do negócio, no entanto, considerando que atualmente a controladoria e toda a custódia dos fundos geridos pela HCO são terceirizadas com outras instituições autorizadas a prestar esses serviços pela CVM, a continuidade das atividades da HCO em caso de desastres, interrupção parcial de acesso às instalações físicas ou restrição de acesso aos recursos tecnológicos deve ser garantida conforme abaixo:

I. Energia: o acesso à energia é básico para o funcionamento do escritório da HCO. Assim, as nossas instalações contam com sistema fornecido por rede de energia (Enel) em local com fiação subterrânea (região da Faria Lima, São Paulo) o que previne os incidentes de queda de energia. Adicionalmente, há *nobreak* para as máquinas e servidores para prevenção de quedas espontâneas de energia e surtos de tensão;

II. *Internet*: o acesso é primordial para as consultas de portfólio e cadastros de movimentações no website do controlador terceirizado. A contingência primária é dada por sistema fibra contratado por empresa de telefonia de grande porte;

III. Restrição de Acesso Físico: em caso de indisponibilidade de acesso às instalações físicas, o plano de trabalho deve ser feito via acesso à internet existente nas residências de seus sócios e funcionários, acesso as informações via sistema Cloud Computing;

IV. *E-mail*: o acesso ao correio eletrônico corporativo de domínio www.hcogroup.com.br, também é uma ferramenta primordial para continuidade dos serviços da HCO. Pensando nisso, a HCO usa a tecnologia disponível da Microsoft, com correio eletrônico em "nuvem".;

V. Telefonia: a telefonia celular própria dos funcionários também pode ser utilizada para solução básica de contingência;

VI. Acesso aos Arquivos: o acesso aos arquivos ocorre através de servidor em nuvem com sistema de contingência em nuvem, de forma que tais discos possam ser facilmente acessados via computadores pessoais de sócios e funcionários da HCO;

VII. Backups: os backups são realizados todos os dias com retenção em disco por 1 (uma) semana. No último domingo de cada mês, 2 (duas) cópias completas de todos os arquivos são realizadas e armazenadas, a primeira em uma área reservada dentro das dependências da HCO e a segunda em mídia localizada fora das referidas dependências; e

VIII. Restauração dos Sistemas: a área administrativa, junto ao departamento de tecnologia, é responsável por manter disponível toda a documentação necessária, bem como todos os dados e softwares necessários para a restauração dos sistemas.

20. SERVIÇOS TERCEIRIZADOS (DILIGÊNCIA NA CONTRATAÇÃO DE PRESTADORES DE SERVIÇOS)

20.1. A HCO pode, deliberadamente, a seu exclusivo critério, terceirizar serviços desde que garanta, também com base em sua "Política de Seleção, Contratação e Supervisão de Prestadores de Serviços", que os prestadores contratados: **(i)** apresentem toda documentação necessária em conformidade com os padrões da HCO; **(ii)** possuam procedimentos e controles adequados ao ambiente regulatório e práticas de mercado; **(iii)** possuam reputação e imagem íntegras e idôneas; e **(iv)** possuam infraestrutura adequada à prestação dos serviços objeto de sua contratação, a fim de assegurar, entre outros, que os respectivos serviços não sejam interrompidos em caso de eventuais indisponibilidades.

21. AUSÊNCIA TEMPORÁRIA DOS DIRETORES ESTATUTÁRIOS

21.1. Conforme especificado no Estatuto Social da HCO, o Sr. **Ariel Araújo de Almeida** consiste no único Diretor responsável pela Área de Gestão da instituição e a Sra. **Manuela Siqueira Aguiar Précaro** consiste na única Diretora responsável pela Área de *Compliance* e Risco da instituição. Em situações emergenciais e de contingências operacionais, tanto o Sr. Ariel quanto a Sra. Manuela poderão ser substituídos pelos respectivos profissionais de backup de suas áreas, em observância às determinações do Guia para Habilitação de Pessoa Jurídica da ANBIMA.

21.2. Observadas as disposições do item 21.1 acima, a diretoria também terá poderes para nomear quantos procuradores forem necessários para a representação da empresa, sendo que as procurações lavradas para tal fim deverão especificar os poderes e o prazo do mandato, com exceção dos procuradores judiciais, que poderão atuar por tempo indeterminado. A representação passiva e ativa da HCO, em juízo ou fora dele, deverá observar as determinações do Estatuto Social.

22. PLANO DE AÇÃO

22.1. Em algumas situações de contingência, será necessário adotar as medidas abaixo:

Impossibilidade de Acessar a Sede da HCO:

I. entrar em contato com o gestor da respectiva área e verificar como proceder; e

II. se tiver subordinados, entrar em contato e indicar-lhes como proceder; além de acessar o grupo da HCO no Whatsapp para mais informações.

Necessidade de Evacuação:

22.2. O edifício onde está localizada a HCO possui plano de evacuação, e este deverá ser respeitado.

Testes e Apuração na Qualidade da Estrutura de Contingência:

22.3. O departamento de *compliance* é responsável, com o auxílio da área de tecnologia, por organizar, coordenar e supervisionar testes de contingência periódicos. Nesses testes, todos os procedimentos devem ser executados em sua integridade, a fim de identificar os pontos falhos na contingência e aprimorá-los.

22.4. Periodicamente, são realizados testes efetivos da estrutura de *backup* e realizados quaisquer ajustes que se tornem necessários.

22.5. Cabe às áreas envolvidas garantir que quaisquer mudanças/ajustes necessários sejam realizados em tempo hábil.

23. TREINAMENTO

23.1. A HCO possui um processo de treinamento inicial e um programa de reciclagem contínua dos conhecimentos sobre as políticas internas, inclusive este Manual, aplicável a todos os Colaboradores, especialmente àqueles que tenham acesso à Informações Confidenciais e/ou participem do processo de decisão de investimento.

23.2. O Diretor de *Compliance* e Risco deverá conduzir sessões de treinamento aos Colaboradores periodicamente, conforme entender ser necessário, de forma que os Colaboradores entendam e cumpram as disposições previstas neste Manual, e deve estar frequentemente disponível para responder questões que possam surgir em relação aos termos deste Manual e quaisquer regras relacionadas à *compliance*.

23.3. A periodicidade mínima do processo de reciclagem continuada será anual. A cada processo de reciclagem continuada, os Colaboradores assinarão termo comprovando a participação no respectivo processo.

23.4. Os materiais, carga horária e grade horária serão definidos pelo Diretor de *Compliance* e Risco, que poderá, inclusive, contratar terceiros para ministrar aulas e/ou palestrantes sobre assuntos pertinentes.

24. DEFINIÇÕES

24.1. Para o perfeito entendimento deste Manual, faz-se necessário definir o significado de alguns termos mencionados, são eles:

I. Antivírus: programa que detecta e elimina vírus de computador;

II. Ativos: todo e qualquer bem material pertencente ou gerido pela HCO, que podem ser:

A. Ativos de Informação: base de dados e arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas etc.;

B. Ativos de Software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários; e

C. Ativos Físicos: equipamentos computacionais (computadores, processadores, monitores, *laptops*, *modems* etc.), equipamentos de comunicação (roteadores, PABX, telefones fixos etc.), mídias (fitas e discos magnéticos, discos ópticos etc.), outros equipamentos técnicos (*no-breaks*, aparelhos de ar-condicionado etc.), mobília, acomodações etc.;

III. Backup: cópia exata de um programa, disco ou arquivo de dados feito para fins de arquivamento ou para salvaguardar informações;

IV. Cavalo de Tróia: programa que pode danificar áreas da máquina e torná-la vulnerável ao ataque de *hackers*;

V. Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

VI. Controle de Acesso: conjunto de restrições ao acesso às informações de um sistema exercido pela equipe de segurança da informação;

VII. Criptografia: arte/ciência de utilizar matemática para tornar a informação segura, criando um grande nível de confiança no meio eletrônico;

VIII. Direito de Acesso: privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

IX. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

X. *Download*: transferência de arquivo de um computador remoto para outro computador através da rede;

XI. Ferramentas: conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades;

XII. *Handheld*: computadores que cabem na palma da mão (*palmtops*) e que tem recursos para organização pessoal e comunicação móvel;

XIII. Incidente de Segurança: qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade ou disponibilidade de qualquer ativo;

XIV. Integridade: salvaguarda da exatidão da informação e dos métodos de processamento;

XV. *Junk Mail*: *e-mails* não solicitados por usuários não interessados em recebê-los;

XVI. *Log*: registro das transações ou atividades realizadas em sistema de computador;

XVII. *No-Break*: sistema com baterias que mantém o computador funcionando por um determinado período;

XVIII. *Peer-to-Peer*: rede por meio da qual usuários compartilham entre si seus recursos, possibilitando a provisão de conteúdos e serviços à rede;

XIX. Política de Segurança: conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos sistemas de informação;

XX. Proteção dos Ativos: processo pelo qual os ativos devem receber classificação quanto ao respectivo grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

XXI. Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação;

XXII. Senha Fraca ou Óbvia: senha que utiliza caracteres de fácil associação ao seu dono, que seja muito simples ou pequena, tais como datas de aniversário, casamento, nascimento, o próprio nome do usuário, nome de seus familiares, sequências numéricas simples, palavras com significado, dentre outras;

XXIII. *Spam*: *e-mail* não solicitado enviado a um grande número de endereços eletrônicos, que geralmente visam fazer propaganda de produtos e serviços; e

XXIV. Vírus: programa construído para causar danos aos *softwares* do computador.

25. CONSIDERAÇÕES FINAIS

25.1. O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar o departamento de *compliance*.

25.2. O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar à demissão ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicáveis.

25.3. Este Manual deverá ser revisado quando mudanças significativas ocorrerem na legislação aplicável ou nos processos internos da HCO, para assegurar a sua contínua relevância, conformidade e aplicabilidade.

ANEXO I
Termo de Adesão ("Termo de Adesão")

Eu, [•], portador(a) da Cédula de Identidade RG nº [•] e/ou Carteira de Trabalho e Previdência Social nº [•], série [•], declaro para os devidos fins que:

I. estou ciente da existência do "Manual de *Compliance* e Controles Internos" da HCO Group S.A. ("Manual" e "HCO", respectivamente) e de todas as políticas internas da HCO, inclusive o "Código de Ética", a "Política de Negociação" e a Política de Gestão de Risco (em conjunto, "Políticas Internas"), que recebi, li e tenho em meu poder;

II. tenho ciência do inteiro teor do Manual e das Políticas Internas, com os quais declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Manual), junto às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas pela HCO, e comprometo-me a comunicar, imediatamente, aos diretores da HCO qualquer quebra de conduta ética das regras e procedimentos que venha a ser de meu conhecimento, seja diretamente ou por terceiros;

III. tenho ciência e comprometo-me a observar integralmente os termos da Política de Confidencialidade estabelecida no Manual da HCO, sob pena da aplicação das sanções cabíveis, nos termos do item IV abaixo;

IV. o não-cumprimento do Código de Ética e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigo-me a ressarcir qualquer dano e/ou prejuízo sofridos pela HCO e/ou os respectivos sócios e diretores, oriundos do não cumprimento do Manual e/ou das Políticas Internas, sujeitando-me à responsabilização nas esferas civil e criminal;

V. participei do processo de integração e treinamento inicial da HCO, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades e da HCO, notadamente àquelas relativas à segregação de atividades, e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas, de modo que as compreendi e me comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento continuado;

VI. as normas estipuladas no Manual e nas Políticas Internas não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de qualquer outra

norma mencionada pela HCO, mas servem de complemento e esclarecem em como lidar em determinadas situações relacionadas à minha atividade profissional;

VII. autorizo a divulgação de meus contatos telefônicos aos demais Colaboradores, sendo que comunicarei à HCO a respeito de qualquer alteração destas informações, bem como de outros dados cadastrais a meu respeito, tão logo tal modificação ocorra; e

VIII. Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado. A seguir, informo as situações hoje existentes que, ocasionalmente, poderiam ser enquadradas como infrações ou conflitos de interesse, de acordo com os termos do Manual, salvo conflitos decorrentes de participações em outras empresas, descritos na Política de Negociação, os quais tenho ciência que deverão ser especificados nos termos previstos no Manual:

[Local], [•] de [•] de 20[•].

_____

[Assinatura]