POLITICA
Português - Brasil

MANUAL DE COMPLIANCE

PROPÓSITO

O objetivo desta política é estabelecer e manter os padrões e diretrizes do Manual de Compliance da HDB Gestão.

ESCOPO

A Política e as Diretrizes se aplicam a todos os funcionários da HDB Gestão.

HDB GESTÃO

INTRODUÇÃO

O presente Manual de Compliance ("Manual") visa assegurar, por meio de um controle interno adequado, o cumprimento permanente das regras, políticas e regulamentos atuais relacionados aos diferentes tipos de investimentos e à atividade de gestão de carteiras de valores mobiliários da **HDB Gestão e Consultoria Imobiliária Ltda.** ("HDB Gestão" ou "Gestora") no exercício de suas atividades de gestão de recursos de terceiros e/ou consultoria de valores mobiliários, de acordo com a Resolução CVM nº 21, de 21 de fevereiro de 2021, conforme alterada ("Resolução CVM 21").

Este Manual deve ser lido em conjunto com o Código de Ética e as demais políticas da Gestora, observado que todos os termos iniciados em letra maiúscula que não forem aqui definidos têm seu significado atribuído no Código de Ética da HDB Gestão.

Este Manual será aplicável a todos os profissionais empregados pela HDB Gestão envolvidos nas áreas de Gerenciamento de Recursos, Controles Internos e Compliance da HDB Gestão, incluindo sem limitação qualquer sócio, diretor, conselheiro, gerente, empregado, trainee e estagiário, bem como outras pessoas que possuam status similar ou desempenhem funções similares ("Colaboradores HDB").

DEFINIÇÕES

Todos os termos iniciados em letra maiúscula que não forem aqui definidos têm seu significado atribuído no Código de Ética da HDB Gestão.

PROTEÇÃO DAS INFORMAÇÕES DE PROPRIEDADE EXCLUSIVA DA EMPRESA E DO INVESTIDOR

Procedimentos para a Divulgação Adequada de Informações

À luz das disposições de confidencialidade estabelecidas neste Manual, salvo se adequado no contexto de suas responsabilidades profissionais, um Colaborador HDB não poderá revelar a qualquer pessoa não associada à HDB Gestão (exceto: (i) àqueles envolvidos em uma operação ou com direito às informações em nome de um investidor; (ii) àqueles que prestem serviços jurídicos, contábeis, administrativos ou outros serviços ao respectivo fundo ou correntista;

(iii) conforme exigido por lei ou por ordem de autoridades governamentais; ou (iv) especificamente solicitado por tal investidor) qualquer informação relativa aos investidores, incluindo dados pessoais fornecidos à HDB Gestão por qualquer investidor; Listas e arquivos de investidores ou outras informações do investidor; registros comerciais da HDB Gestão, informações de empregados, informações financeiras, software, licenças, contratos, arquivos de computador e planos de negócios; modelos, pesquisa de propriedade exclusiva, direitos autorais ou outros materiais pagos por um fundo ou pela HDB Gestão; e as análises e outros dados ou informações de propriedade exclusiva da HDB Gestão. Todas essas informações, sejam ou não materiais, são estritamente confidenciais e não podem ser divulgadas. Os Colaboradores HDB também não violarão as disposições de qualquer acordo de confidencialidade do qual a HDB Gestão ou o Colaborador HDB seja parte.

Quaisquer comunicações recebidas de autoridades governamentais, reguladoras ou autorreguladoras, devem ser prontamente encaminhadas ao Diretor de Compliance para o tratamento adequado.

Os Colaboradores HDB não poderão divulgar informações relativas a recomendações ou possíveis operações que ainda não estejam assinadas ou que estejam sendo consideradas, exceto (i) conforme seja necessário; ou (ii) conforme exigido por lei (nesse caso, mediante notificação ao Diretor de Compliance – a notificação ao Diretor de Compliance se dá a partir da plataforma para o gerenciamento de Compliance denominada mycompliance e gerida pelo Grupo Hines); e (v) após a informação estar de outra forma disponível ao público.

A HDB Gestão possui como dever primordial a lealdade a todo e qualquer investidor. Esse dever inclui a não apropriação indevidamente de informações e/ou estratégias desenvolvidas para uso na administração do capital da HDB Gestão com o objetivo de utilizá-las em negociações pessoais (ou negociações para outras contas) de tais Colaboradores HDB. De maneira geral, as políticas de negociações pessoais da HDB Gestão presentes no referido Código de Ética devem evitar tal apropriação indevida, mas caso qualquer Colaborador HDB acredite estar em posição de lucrar com o uso de informações específicas que recebeu ou que foram geradas por conta da gestão dos investimentos da HDB Gestão, tal Colaborador HDB não deverá executar a operação em questão. Assim, indo ao encontro com as políticas internas da HDB Gestão.

TRATAMENTO DE DADOS

Titularidade de Dados

Com exceção do material claramente de propriedade de terceiros, tais como seus dados pessoais confidenciais, a HDB Gestão é a legítima titular de todas as informações comerciais armazenadas ou transmitidas através de seus sistemas. A menos que a HDB Gestão tenha celebrado um acordo específico por escrito, todas as informações comerciais desenvolvidas enquanto um Colaborador HDB estiver empregado pela HDB Gestão são de propriedade da HDB Gestão.

Os Colaboradores HDB, fornecedores e quaisquer outros terceiros não poderão copiar os softwares e/ou arquivos fornecidos pela HDB Gestão para qualquer meio de armazenamento, transferir tal software e/ou arquivo para outro computador ou divulgar tal software e/ou arquivo a terceiros externos sem permissão prévia do Diretor de Compliance.

CONTROLE DE ACESSO À INFORMAÇÃO

A HDB Gestão utiliza alguns mecanismos para garantir o controle de acesso a todas as suas informações e base de dados, conforme a seguir:

Senha para acesso:

Todos os computadores e dispositivos que acessem o e-mail e/ou dados da HDB Gestão devem ter uma senha definida para todas as contas de usuário, incluindo de qualquer Colaborador HDB, e devem ser configurados para bloquear automaticamente a tela quando deixados sem supervisão após um determinado período. A HDB Gestão poderá, a seu critério, limitar a capacidade de um empregado ou de um destinatário de imprimir, encaminhar ou salvar um documento.

Criptografia:

A HDB Gestão poderá utilizar software de criptografia que permita aos Colaboradores HDB garantir a segurança dos dados da HDB Gestão através do uso de e-mail e outros métodos de transmissão.

Acesso Remoto e Dispositivo Móveis:

Todas os Colaboradores HDB podem acessar a rede da HDB Gestão de forma remota. A HDB Gestão reserva o direito de conduzir inspeções surpresa dos usuários com privilégios de acesso remoto visando à proteção e segurança dos dados e informações da HDB Gestão.

O acesso remoto, pela sua natureza, tem um nível de risco inerentemente mais elevado. O acesso remoto aos sistemas HDB Gestão está disponível de diversas maneiras, dependendo do

dispositivo que o Colaborador HDB está utilizando e das necessidades do seu trabalho. Isso inclui aplicativos da web, serviços de área de trabalho remota e VPN.

A Intranet da HDB Gestão está disponível apenas para Colaboradores HDB e determinados parceiros de extranet de acordo com a necessidade.

Outros aplicativos baseados na web estão disponíveis para funcionários e parceiros de extranet conforme a necessidade.

O acesso dos Serviços de Área de Trabalho Remota a aplicativos e serviços está disponível para Colaboradores HDB e parceiros de extranet com base na necessidade.

O acesso VPN completo está disponível apenas para Colaboradores HDB que usam um computador gerenciado pela HDB Gestão, e o computador deve estar executando aplicativos antimalware e firewall aprovados atualmente.

A VPN limitada está disponível para não funcionários onde suas responsabilidades exigem tal acesso.

Solicitações de acesso remoto: O acesso remoto é permitido aos Colaboradores HDB desde que sejam utilizados os métodos de conexão e os dispositivos necessários. Quando o acesso remoto for necessário para qualquer não funcionário, esse acesso só poderá ser fornecido após aprovação do Diretor de Segurança da Informação, Diretor Sênior - Segurança e Conformidade da Informação (CISO).

Dispositivos de acesso remoto aprovados: Equipamentos fornecidos pela HDB podem ser usados para estabelecer conexões de acesso remoto. Além disso, equipamentos de propriedade do usuário que tenham sido autorizados pela TI para uma finalidade comercial específica poderão ser usados; caso contrário, os equipamentos de propriedade do usuário não poderão ser usados para conectividade VPN; entretanto, esses dispositivos podem se conectar por meio de outros métodos mencionados anteriormente. Computadores pessoais domésticos não gerenciados pelo time de tecnologia da informação da HDB Gestão (“HDB IT”) e, portanto, não podem ser garantidos que estejam protegidos pelos padrões de segurança corporativa da Hines. Eles são considerados dispositivos inseguros. Os dados da Hines não devem ser armazenados em nenhum dispositivo inseguro.

Acesso remoto à rede local: os dispositivos que se conectam remotamente à rede local (LAN) devem cumprir o seguinte:

● Todos os computadores conectados a redes internas através de tecnologias de acesso remoto devem ter um sistema operacional

atualizado e proteção de endpoint aprovada e atualizada;

● A autenticação de dois fatores é necessária antes que o acesso à rede possa ser concedido (consulte a Seção: SEGURANÇA LÓGICA – Autenticação multifator).

Controle remoto de dispositivos: somente tecnologia e software de controle remoto de dispositivos aprovados pela TI podem ser usados para controlar remotamente um servidor, computador, smartphone, aplicativo, etc., e somente sob as seguintes condições:

● O Controle Remoto só será usado como uma ferramenta para conexão com o próprio computador de trabalho, para cumprir as próprias responsabilidades profissionais.

● O procedimento para o pessoal de Tecnologia da Informação acessar/controlar remotamente a estação de trabalho de outra pessoa é entrar em contato com o usuário da estação de trabalho por telefone para notificá-lo sobre o acesso necessário.

● O uso de software de controle remoto para acessar o computador de outra pessoa é limitado ao pessoal autorizado de Tecnologia da Informação e aos prestadores de serviços terceirizados autorizados.

Acesso Remoto para Diagnóstico/Manutenção: todas as conexões de acesso remoto para diagnóstico e manutenção de equipamentos devem ser configuradas de forma a garantir a conformidade com o acesso remoto.

O acesso às redes por meio de mecanismos de comunicação sem fio não seguros é estritamente proibido. Os Colaboradores HDB só podem conduzir negócios da HDB Gestão e conectar-se à rede sem fio dos Colaboradores HDB usando dispositivos seguros e autorizados pela HDB Gestão, gerenciados por meio da plataforma de gerenciamento de dispositivos móveis (MDM) da HDB Gestão. Dispositivos externos, como os usados pelos visitantes, só podem se conectar à rede sem fio do Convidado. Dispositivos sem fio pessoais que não estejam inscritos no programa BYOD não poderão ser usados para negócios da empresa.

Todos os dispositivos de computação móvel que acessam o sistema de e-mail da Hines são forçados a se inscrever no sistema MDM da Hines, o que, por sua vez, faz com que os dispositivos cumpram os seguintes padrões:

Padrões de segurança de dispositivos móveis (aplicados pela plataforma MDM da Hines):

● Proteção por senha – Qualquer dispositivo móvel que acesse os dados da Hines deve ter uma senha definida para poder usar o

dispositivo.

● O recurso de limpeza remota é necessário para qualquer dispositivo que acesse o sistema de e-mail da Hines. Os dispositivos serão imediatamente apagados remotamente em caso de perda ou roubo do dispositivo.

● Tempo limite máximo de segurança – O dispositivo será bloqueado automaticamente após 60 minutos de inatividade, a menos que o usuário especifique um período mais curto, como 10 ou 30 minutos (recomendado pela TI).

● Configurações de senha.

● A criptografia será ativada se o dispositivo for capaz disso.

Armazenamento móvel:

Devido à natureza portátil das mídias de computador, como CDs, DVDs, discos rígidos removíveis, unidades flash USB, etc., esses dispositivos são considerados inseguros, a menos que sejam criptografados. Para dispositivos utilizados por funcionários que possam ter acesso a informações privilegiadas, o uso de dispositivos de armazenamento USB pode ser desativado por meio da Política do Grupo Hines.

Programas Antivírus:

No âmbito deste Manual, a HDB Gestão atualizará os sistemas operacionais e software em sua rede quando necessário; tais atualizações ajudarão a reduzir as vulnerabilidades da rede, uma vez que as atualizações frequentemente abordam ameaças conhecidas ou antecipadas.

A HDB Gestão monitorará regularmente eventos e conexões através do *firewall* da HDB Gestão para detectar quaisquer violações, ataques ou acesso a informações sensíveis. A HDB Gestão garantirá que softwares antivírus sejam instalados em todos os computadores, que o acesso ao servidor seja definido e periodicamente auditado e que privilégios de administrador sejam implementados.

Equipamentos Extraviados

Caso um computador laptop ou dispositivo móvel seja extraviado ou roubado, ou esteja fora do controle de um empregado por mais de 24 (vinte e quatro) horas, o empregado deverá notificar o setor de tecnologia, que tomará as devidas precauções para desativar as informações para o laptop ou dispositivo móvel. Além disso, todos os computadores, laptops, *tablets* e telefones celulares dos empregados são criptografados, tornando os dados ilegíveis em caso de perda ou

roubo.

Acesso à internet e redes sem fio:

O acesso à Internet é fornecido para a HDB Gestão e é considerado um recurso para a HDB Brasil. O acesso à Internet fornecido pela HDB Gestão não deve ser usado para entretenimento, tão somente como ferramenta de pesquisa e trabalho.

Os nomes e senhas das redes sem fio estão sujeitos a alterações por razões de segurança a qualquer momento, com pouca ou nenhuma notificação. A HDB Gestão implementou pontos de acesso sem fio para conceder acesso exclusivamente aos recursos da Internet. Os dispositivos e usuários nesta rede são separados por um firewall dos recursos internos da rede. Os usuários finais estão proibidos de instalar pontos de acesso sem fio para sua própria conveniência. Os pontos de acesso sem fio devem ser protegidos.

Nenhum ponto de acesso sem fio pode ser conectado à Rede Global da Hines sem aprovação expressa por escrito da Hines IT. Qualquer ponto de acesso sem fio aprovado deve ser configurado de acordo com as especificações atuais de configuração de TI da Hines. Qualquer ponto de acesso sem fio que não esteja registrado na Hines IT ou não esteja configurado corretamente será desconectado imediatamente da Hines Global Network.

Detalhes adicionais da rede sem fio:

- O acesso sem fio é separado em duas redes distintas o Hines_Internal; e

- Hines_Guest: o acesso é controlado por WPA2 e protegido por senha.

SEGURANÇA CIBERNÉTICA (CIBERSEGURANÇA)

Um incidente de segurança cibernética é qualquer evento, violação de controle ou mau funcionamento de software que possa representar uma ameaça à confidencialidade, integridade ou disponibilidade de sistemas, aplicativos ou informações de suporte. Todos os incidentes de segurança cibernética devem ser imediatamente relatados à TI. (O pessoal de TI DEVE relatar imediatamente cada incidente ao Diretor de Segurança da Informação, Diretor Sênior - Segurança e Conformidade da Informação (CISO). A notificação inicial do incidente pode ser fornecida pessoalmente, por e-mail ou por telefone; no entanto, a TI deve documentar imediatamente o incidente em um tíquete de central de serviços. O gerenciamento de TI avaliará o incidente e determinará o curso de ação apropriado.

Seguro de cibersegurança

A Hines mantém seguro de segurança cibernética para mitigar qualquer impacto financeiro negativo ou perturbador de um problema cibernético.

Avaliação de ameaças e vulnerabilidades

As empresas usam uma variedade de informações em seu processo de avaliação de risco. No que diz respeito às ameaças, estas informações incluem incidentes de segurança cibernética anteriores, quer na empresa, quer observados na indústria, informações sobre ameaças identificadas por outras organizações ou através de organizações de segurança, como o Centro de Análise e Partilha de Informações de Serviços Financeiros (FS-ISAC). Essas ameaças podem incluir ameaças internas – por exemplo, ameaças de funcionários – ou ameaças externas, como hacktivistas ou grupos do crime organizado. Outro componente importante do processo de avaliação de riscos é a análise de vulnerabilidades – o processo de identificação, quantificação e priorização de vulnerabilidades potenciais dentro de um sistema. A sofisticação da análise de vulnerabilidade varia entre as empresas. Uma abordagem comumente usada é o *Common Vulnerability Scoring System* (CVSS) para avaliar vulnerabilidades em aplicativos. CVSS é um padrão aberto do setor para avaliar a gravidade das vulnerabilidades e priorizar sua correção. Os resultados destas revisões são utilizados como contributos para o programa de avaliação de risco da empresa e orientariam as classificações de risco de vários ativos críticos.

Equipe Corporativa de Resposta a Incidentes Cibernéticos (C-CIRT)

O C-CIRT tem a responsabilidade de supervisionar a remediação e resolução de incidentes cibernéticos materiais a nível corporativo. O C-CIRT é presidido pelo Diretor de Tecnologia (CTO) e composto por partes interessadas de departamentos importantes, como TI, Jurídico, Recursos Humanos, Comunicações Corporativas, Gestão de Riscos, Operações Corporativas e Serviços de Engenharia, Escritório de Estratégia Digital Global e Conformidade Corporativa.

É responsabilidade do C-CIRT determinar se a administração executiva, o conselho, o regulador, o cliente ou as autoridades legais exigem a notificação de um Incidente de Alto Nível. Na medida em que a divulgação seja exigida, é responsabilidade do C-CIRT coordenar tal divulgação. O C-CIRT deve cumprir os requisitos legais para notificação de incidentes críticos de segurança às agências reguladoras e governamentais, incluindo agências de aplicação da lei e/ou partes afetadas.

Equipe de Resposta a Incidentes Cibernéticos de Tecnologia da

Informação (IT-CIRT)

O IT-CIRT tem a responsabilidade de supervisionar a remediação e resolução de incidentes cibernéticos materiais a partir do nível de TI. O IT-CIRT é presidido pelo Chefe de Segurança da Informação Diretor (CISO) e composto pelos Chefes de cada Vertical de TI, o Chefe de Infraestrutura de TI e diversos membros de TI (dependendo do tipo de incidente).

É responsabilidade do IT-CIRT conter, interromper e remediar o evento técnico (ou ataque), determinar o impacto do sistema, determinar se ocorreu divulgação ou uso não autorizado de informações pessoais, realizar uma análise de causa raiz e remediar causa raiz. O IT-CIRT comunicará o status e o progresso ao C-CIRT durante todo o processo.

Alertas de dispositivos de segurança de rede

Conforme apropriado, alertas de dispositivos de segurança de rede, incluindo, entre outros, firewalls, detecção de intrusão ou tecnologias de prevenção, devem ser coletados em conjunto com qualquer investigação de um Incidente de Segurança da Informação.

Revisão do Processo de Resposta a Incidentes Cibernéticos

O Plano de Resposta a Incidentes Cibernéticos é continuamente revisado e atualizado, pelo menos anualmente, para garantir que o plano seja consistente e viável com quaisquer mudanças nas reestruturações organizacionais, níveis de pessoal, tendências do setor e avaliações de risco. Um exercício de "*Lições Aprendidas*" é realizado no final de uma resposta real a um incidente, e exercícios de mesa periódicos garantem que cada departamento de partes interessadas especializado no assunto esteja ciente de suas responsabilidades e capacidades.

Escalação de Incidentes

● Qualquer impacto material ou potencial impacto material deve ser encaminhado imediatamente ao CISO.

● O CISO avaliará e classificará a materialidade do impacto ou impacto potencial e determinará se o IT-CIRT é necessário e se o C-CIRT precisa ser notificado e convocado para nova escalada.

● O CISO ou Diretor de Tecnologia (CTO) reportará semestralmente (ou conforme solicitado) ao Comitê de Auditoria e/ou ao Comitê de Pessoas e Infraestrutura (P&I) o status e as tendências dos incidentes.

● Os incidentes materiais também serão coordenados com o IT-CIRT e o C-CIRT, de acordo com as políticas e processos de escalonamento.

● Incidentes considerados não materiais ou de baixo nível não serão

comunicados ao C-CIRT.

● Todos os incidentes serão remediados com uma prioridade adequada ao impacto e em relação a quaisquer outros incidentes abertos.

Requisitos de informações para relatórios de incidentes

Um relatório de incidente deve incluir:

● Detalhes de contato do notificador de incidentes — Área funcional, nome, telefone

● Data e hora do incidente

● Data e hora da resolução

● Tipo de incidente

● Tipo de dados envolvidos

● Causa raiz

● Classificação de Gravidade - Alta, Média, Baixa

● Descrição do Incidente (incluir a fonte do incidente, se conhecida, mas não deve incluir a identificação de qualquer indivíduo específico)

● Impacto do Incidente (real ou potencial)

● Resolução de Incidente (ação de resolução e prevenção de recorrência)

● Informações técnicas (conforme listadas no formulário)

● Conforme apropriado, quaisquer alterações necessárias na infraestrutura, software ou controles para evitar um futuro incidente semelhante.

Tipos de Incidentes

A descrição dos tipos de incidentes inclui, mas não está limitada ao seguinte:

● Violação da política

● Fraqueza de segurança

● Comprometimento da conta

● Vulnerabilidade comportamental

● Corrupção de dados/informações

● Negação de serviço

● Divulgação (uso indevido) de dados/informações

● Comprometimento da rede

● Comprometimento de senha

● Segurança física

● Sondas (não autorizadas)

● Violações de políticas

● Roubo — Dados

● Roubo — Físico

● Acesso e/ou uso não autorizado

● Vírus (sem quarentena)

● Violação de segurança em fornecedores terceirizados críticos

Objetivo e Escopo

A intenção do Plano de Resposta a Incidentes Cibernéticos (CIRP) é fornecer um processo estabelecido sobre como responder a um incidente de segurança da informação. Este plano não é uma lista de verificação passo a passo exaustiva, mas uma visão geral das fases e da ordem de ações de alto nível. Este plano entende que cada departamento especializado no assunto mantém seu próprio plano de resposta a incidentes, sejam eles relacionados à segurança da informação ou não, e, portanto, depende de seus respectivos planos de resposta para lidar com suas atividades de resposta específicas. O plano a seguir foi concebido principalmente a partir de uma perspectiva de TI, com a intenção não de ser um guia abrangente para todas as atividades de resposta a incidentes cibernéticos, mas de ser o guia geral e o catalisador para ativar os planos de resposta diferentes e específicos de cada especialista no assunto e parte interessada. departamentos. Este plano de resposta a incidentes aborda todos os incidentes relacionados à segurança cibernética, sejam eles ocorridos no ambiente corporativo da Hines ou em um ativo/edifício individual da Hines.

Fases de Resposta a Incidentes Cibernéticos

Embora os detalhes da resposta a cada incidente variem muito, o esboço geral pode ser visto nas fases seguintes.

1. Identificação

2. Remediação

3. Acompanhamento e Lições Aprendidas

4. Atualizar o plano de resposta a incidentes cibernéticos (inclui

informar a todos sobre as atualizações)

5. Atualizações periódicas do plano, testes, exercícios de mesa, etc.

Visão geral da resposta a incidentes cibernéticos

A seguir está uma visão geral de alto nível do processo de resposta a incidentes cibernéticos. Cada etapa pode ter muitas subetapas, embora essas subetapas não sejam descritas neste documento.

1. Notifique a gestão de TI assim que um problema cibernético for identificado. a. O método específico para notificar o gerenciamento de TI não é tão importante quanto a notificação ocorrer assim que um incidente potencial for identificado.

2. A gestão de TI avaliará se o problema é de facto um incidente e se requer escalonamento.

3. Se for necessário um escalonamento, o CISO ativará o IT-CIRT e notificará o C-CIRT.

4. O IT-CIRT continua a avaliar e remediar o incidente. Os esforços de remediação incluem não apenas interromper o incidente, mas também podem incluir isolar ou “bloquear” outras áreas ou sistemas para evitar a propagação do incidente, determinar o impacto do sistema, determinar se ocorreu divulgação ou uso não autorizado de informações pessoais, análise da causa raiz, remediação de causa raiz.

5. Cada membro do C-CIRT avalia o impacto na sua área de responsabilidade e inicia o nível apropriado de ação, resposta, inclusão de recursos adicionais, comunicação, escalonamento, etc.

6. A TI comunica periodicamente o status aos usuários afetados e ao gerenciamento de TI, bem como recomenda soluções provisórias para minimizar a interrupção dos negócios. Consulte o palavreado “Alerta de segurança cibernética” abaixo.

7. Quando apropriado, um Relatório de Resposta a Incidentes Cibernéticos será emitido para a Gestão de TI e para a Força-Tarefa de Segurança Cibernética, documentando o evento e as ações de remediação.

8. A gestão de TI avalia se deve envolver o seu parceiro externo de resposta a incidentes cibernéticos, tendo em conta, entre muitos fatores, o âmbito do incidente, a capacidade dos recursos internos para conter e remediar o incidente, o tempo esperado necessário para remediar o incidente, o risco de interrupção dos negócios, o risco de dados comprometidos, etc.

9. As atualizações de comunicação com o IT-CIRT e o C-CIRT ocorrem

regularmente durante todas as fases de resposta a incidentes.

10. Se apropriado, envolver o parceiro externo pré-estabelecido de resposta a incidentes cibernéticos da Hines.

11. Siga as instruções do parceiro de resposta a incidentes. Remediação completa do incidente.

12. Se for descoberto qualquer uso ou divulgação não autorizada de informações pessoais, o departamento de Compliance determinará as próximas etapas e os requisitos de relatório.

13. Os vários departamentos especializados no assunto representados no C-CIRT são responsáveis por itens específicos de suas áreas, como interface de conformidade com as agências reguladoras apropriadas, interface de gerenciamento de risco com o(s) provedor(es) de seguro cibernético, comunicações corporativas, tratamento de comunicados de imprensa, etc.

14. A Gestão de TI e o IT-CIRT reúnem-se para discutir todo o evento, a causa raiz, as lições aprendidas, as adições necessárias à infraestrutura ou outros controles e quaisquer atualizações no plano de resposta a incidentes cibernéticos.

15. Cada departamento especializado no assunto se reúne para discutir as lições aprendidas e quaisquer atualizações em seus respectivos processos.

16. O C-CIRT reúne-se novamente para discutir os resultados, as lições aprendidas, quaisquer atualizações necessárias no processo de resposta a incidentes cibernéticos, etc.

CONFIDENCIALIDADE

Os Colaboradores HDB tratarão como confidencial e não revelarão ou divulgarão em circunstância alguma, independentemente da forma em que tais informações sejam divulgadas, comunicadas ou mantidas, qualquer documento ou informação relacionada à HDB Gestão e os fundos geridos por ela, seus investimentos potenciais e efetivos, seus investidores, clientes e prestadores de serviços, incluindo, mas não se limitando a, negociações, métodos, modelos, senhas, pesquisas, arquivos de computador, informações e registros financeiros, programas de software de computador, acordos e/ou contratos, políticas, práticas, conceitos e estratégias de marketing e/ou de criação e métodos de operação, políticas internas, políticas e procedimentos de preços, estimativas de custos, listas de empregados, projeções financeiras ou comerciais, assim como qualquer informação sobre ou recebida de clientes e outras empresas com as quais a HDB Gestão mantenha um relacionamento comercial.

Além disso, no curso de seus negócios, a HDB Gestão celebra acordos de não-divulgação e acordos de confidencialidade com terceiros relacionados a potenciais oportunidades de investimento. A HDB Gestão espera que todos os Colaboradores HDB obedeçam às restrições impostas por esses acordos, incluindo não compartilhar informações de ou sobre essas empresas com qualquer um que não seja funcionário da HDB Gestão.

Não obstante o acima exposto, sempre que uma informação relevante não pública for recebida, os profissionais de investimento da HDB Gestão serão responsáveis por informar ao Diretor de Compliance, para que este possa dar seguimento a todos os procedimentos aplicáveis, bem como dar as devidas recomendações.

Por fim, cada Colaborador HDB é responsável por manter a segurança adequada dos registros da HDB Gestão e de todos os materiais e informações que não se destinam ao conhecimento público. De forma exemplificativa, as seguintes precauções devem ser tomadas por cada Colaborador HDB:

● antes de sair da sede da HDB Gestão, cada Colaborador HDB deve verificar se existem documentos confidenciais nas áreas comuns de trabalho;

● os escritórios individuais devem ser trancados sempre que possível;

● todas as cópias físicas de contratos, cartas de compromisso, documentos de incorporação, documentos de venda, dentre outros, devem ser arquivados em locais com senha assim que razoavelmente possível;

● todos os meios eletrônicos devem ser protegidos adequadamente (por senhas e práticas de gerenciamento de informações) e não devem ser copiados ou compartilhados de maneira inadequada fora ou dentro da HDB Gestão;

● cada Colaborador HDB deve ter um cuidado extra com propostas, licitações, relatórios de gestão, relatórios de locação, relatórios de custos, dentre outros. Cópias físicas desses documentos devem ser mantidas em arquivos trancados sempre que possível.

● qualquer informação potencialmente confidencial não deve ser discutida fora do escritório (ou seja, elevadores, reuniões públicas). Os Colaboradores HDB devem exercer discrição e cautela ao discutir informações confidenciais que possam afetar materialmente uma transação comercial pendente ou resultar em divulgação imprópria de informações materiais não públicas.

● registros financeiros, incluindo demonstrações financeiras auditadas

e não auditadas, estatísticas financeiras, qualquer informação sobre funcionários, manuais, declarações de impostos, diretrizes e manuais operacionais, materiais de treinamento, relatórios de avaliação de propriedade e todos os outros materiais de natureza confidencial, dentre outros, não devem ser distribuídos para qualquer pessoa não autorizada (dentro ou fora da empresa).

● todos os materiais produzidos ou recebidos por um Colaborador HDB e todos os itens contidos nos arquivos do Colaborador HDB são propriedade da HDB Gestão e não devem ser removidos das instalações da HDB Gestão ou usados para fins diferentes dos negócios da HDB Gestão.

TREINAMENTO

Como parte de seu programa de Controles Internos, a HDB Gestão dará treinamento sobre este Manual para todas as Colaboradores HDB e, se necessário, para afiliados e fornecedores. O treinamento pode incluir, entre outros tópicos, instrução sobre a criação de senhas fortes, detecção de e-mails de phishing, dispositivos aprovados, sincronização de dispositivos pessoais e redução da exposição a e-mails. O treinamento ocorrerá periodicamente e sua frequência dependerá de uma série de fatores incluindo, mas não se limitando à evolução das ameaças à segurança. O treinamento pode se dar na forma de reuniões em toda a empresa, distribuição de materiais escritos ou orientação fornecida por e-mail. O Diretor de Compliance será responsável por manter um registro de quaisquer orientações ou materiais escritos fornecidos durante tal treinamento.

Os treinamentos são realizados sempre que o Diretor de Compliance achar necessário e no momento da integração de um novo Colaborador HDB, conforme exposto a seguir:

Treinamento de Integração:

Quando da contratação de um Colaborador HDB e, antes do início efetivo de suas atividades, ele participará de um processo de integração e treinamento onde adquirirá conhecimento sobre as atividades da empresa, regras, políticas e códigos internos, assim como informações sobre as principais leis e regulamentos que regem as atividades da HDB Gestão.

Treinamento contínuo

A HDB Gestão adota um programa anual de reciclagem dos Colabores HDB, a fim de garantir que eles estejam sempre atualizados sobre os termos e responsabilidades aqui descritos, estando todos obrigados a participar de tais programas de reciclagem.

Além disso, no caso de qualquer mudança nas políticas empregadas pela HDB Gestão e/ou da regulamentação aplicável às atividades desenvolvidas pela HDB Gestão, a HDB Gestão poderá conduzir um treinamento a fim de apresentar as mudanças e novos pontos abordados por tal política.

Finalmente, deve-se observar que o processo de treinamento inicial e o programa de reciclagem contínua são desenvolvidos e controlados pelo Diretor de Compliance e exigem o compromisso total dos empregados com seu atendimento e dedicação.

SEGURANÇA DA INFORMAÇÃO

Privacidade dos Empregados

Os Colaboradores HDB não devem ter qualquer expectativa de privacidade ao utilizar os sistemas de informação na HDB Gestão. Para gerenciar sistemas e reforçar a segurança, a HDB Gestão pode registrar, revisar e utilizar qualquer informação armazenada ou que circule através de seus sistemas. A HDB Gestão pode capturar atividades dos usuários como tráfego de e-mail, números de telefone discados e sites visitados. Além disso, a administração da HDB Gestão reserva-se o direito de monitorar, inspecionar ou remover de seus sistemas de informação qualquer material que considere ofensivo ou potencialmente ilegal. Esse exame pode ocorrer com ou sem o consentimento, presença ou conhecimento dos Colaboradores HDB envolvidas. Os sistemas de informação sujeitos a tal exame incluem, mas não estão limitados, a sistemas de correio eletrônico, qualquer dispositivo controlado pela HDB Gestão, arquivos de correio de voz, arquivos de *spool* de impressora, saída de fax, gavetas de mesa e áreas de armazenamento.

Uso Pessoal de Sistemas e Armazenamento de Dados Pessoais

Os sistemas de informação da HDB Gestão são destinados à utilização somente para fins comerciais. Os arquivos pessoais de um Colaborador HDB, tais como documentos, fotos, vídeos ou música, não devem ser armazenados no disco compartilhado da HDB Gestão. O uso pessoal acidental é permitido se não for um risco, não consumir mais do que uma quantidade trivial de recursos que poderiam ser usados para fins comerciais, não interferir na produtividade do usuário e não impedir qualquer atividade comercial. É proibido o uso dos sistemas de informação da HDB Gestão para correspondência em cadeia, solicitações de caridade, material de campanha política, trabalho religioso, transmissão de material questionável, ou qualquer outro uso não comercial. Software pessoal não deve ser instalado nos sistemas de informação da HDB Gestão sem a aprovação expressa do

Diretor de Compliance. A HDB Gestão não é responsável por quaisquer Dados Pessoais armazenados nos computadores ou servidores da empresa e poderá apagar esses dados sem aviso prévio. Além disso, a HDB Gestão não investirá recursos da empresa na recuperação de Dados Pessoais no caso de perda dos mesmos.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

O objetivo do Plano de Contingência e Continuidade de Negócios visa estabelecer as medidas a serem tomadas para evitar um impacto negativo na condução das atividades desenvolvidas pela HDB Gestão, como, por exemplo, crises econômicas nacionais e/ou mundiais, pandemias, falhas operacionais e/ou desastres naturais.

Estratégia de Continuidade de Negócios da Gestora

● Escritório Corporativo e Equipe

A sede corporativa e a equipe da HDB Gestão é localizado em São Paulo, no Brasil. Apesar disso, a HDB Gestão pode utilizar da sede corporativa do Grupo Hines localizada em Houston, Texas (EUA) EUA. O escritório de Houston serve como sede principal para nosso escritório executivo, Comunicações Corporativas, Recursos Humanos, Finanças e Contabilidade, Jurídico, Fiscal, Auditoria Interna, Conformidade, Gestão de Investimentos, Operações Corporativas e Serviços de Engenharia, Sustentabilidade, Hines Advisors/Core Fund, Fund Grupos de Contabilidade e outros departamentos. Estes departamentos, embora vitais para a empresa numa base contínua, não são considerados de missão crítica para a operação diária de back-office do nosso negócio. No caso de um desastre que torne o escritório de Houston inoperante, a equipe trabalhará remotamente em locais dispersos, como residências particulares, hotéis, escritórios de terceiros ou outros locais.

● Departamentos de Missão Crítica

A Hines reconhece que um desastre que destruísse qualquer um de seus escritórios ou instalações de informática representaria um risco operacional significativo. Para mitigar esse risco, a Hines possui políticas e procedimentos que constituem um programa corporativo de continuidade de negócios. O escritório de Houston serve como local principal para nossos departamentos de missão crítica, incluindo: Gestão de Caixa, Serviços Corporativos, Vendas Internas de Mercado de Capitais, Tecnologia da Informação, Folha de Pagamento e Gestão de Risco. Existem planos documentados e testados em vigor para cada um desses departamentos. Redundâncias foram implementadas e testadas para estas funções operacionais críticas.

● Operações globais de data center da Hines

Todas as operações do Hines Global Data Center estão localizadas em um provedor baseado em nuvem. As aplicações são protegidas por servidores redundantes sempre que possível, e os sistemas críticos são hospedados em locais físicos separados dentro da infraestrutura do provedor de nuvem. O parceiro técnico da HDB Gestão também mantém uma infraestrutura secundária de recuperação de desastres no mesmo provedor de nuvem, mas em um local geograficamente diferente. O Parceiro Técnico mantém backups como parte da estratégia operacional do provedor de nuvem. O provedor de nuvem é responsável por garantir o tempo de atividade e as condições operacionais ideais para o hardware que hospeda em nome da Hines e de seu parceiro técnico.

Preparação para o Cenário de Negócios

● Locais de escritórios

Para garantir que a Hines esteja pronta para responder de maneira coordenada a desastres naturais e emergências, recursos estão disponíveis para todos os escritórios para a criação de um plano de contingência e resposta de emergência personalizado e específico para o local, que são testados periodicamente. Se a Hines perder a capacidade de realizar negócios em um dos escritórios, as funções serão realocadas para um local alternativo (por exemplo, outro local, casa, hotel, local de terceiros) em uma área não afetada. Cada local possui planos para essa recuperação e eles são testados periodicamente. Os objetivos do tempo de recuperação variam de acordo com a criticidade de cada função.

Suporte adicional é fornecido às propriedades e regiões pela Equipe Central de Resposta a Crises da Hines, com membros de Operações, Engenharia, Tecnologia da Informação, Gestão de Riscos, Comunicações Corporativas e Recursos Humanos.

● Centro de dados remoto

Se a Hines perder a capacidade de realizar negócios em seu local principal hospedado na nuvem, a Hines IT e seu parceiro técnico farão o failover para seu local de recuperação de desastres. Os planos estão em vigor e são testados pelo menos uma vez por ano.

● Evento Pandêmico

A HDB Gestão tem planos para continuar os negócios durante um evento de pandemia. O plano foi elaborado por uma equipe de funcionários de diversas disciplinas e especialistas em saúde pública com consultoria da International SOS. É um plano de ação multinível

baseado nas orientações da Organização Mundial da Saúde (OMS).

Plano de Delegação de Autoridade

No caso de um desastre ou emergência que resulte na incapacitação de um dos principais líderes seniores, incluindo o Gabinete do CEO, desenvolvemos um Plano de Delegação de Autoridade que garante que pessoal capaz com as habilidades e conhecimentos necessários possa assumir funções conforme necessário e proteger operações de missão crítica. Este Plano de Delegação de Autoridade inclui toda a amplitude da empresa global da Hines. O plano é atualizado anualmente e mantido pelo departamento jurídico. A equipe jurídica facilita conversas com líderes seniores para garantir que a lista seja precisa e reflita as principais necessidades e prioridades. Isto permite-nos estar prontos para ativar uma resposta adequada e oportuna assim que surgir um incidente.

CONTRATAÇÃO E MONITORAMENTO DE TERCEIROS

O objetivo deste dispositivo é estabelecer critérios qualitativos mínimos e orientar o processo de seleção, contratação e monitoramento de indivíduos e entidades que possam ter interesse em iniciar e manter um relacionamento comercial com a HDB Gestão.

Este é um procedimento real de *Know Your Partner* - KYP, focado no conhecimento do terceiro a ser contratado, nos procedimentos de integridade instituídos e observados pelas empresas que operam com a HDB Gestão.

Os critérios e processos aqui estabelecidos visam proporcionar o mínimo indispensável de segurança operacional e jurídica, evitando conflitos de interesse de forma a manter a HDB Gestão em conformidade com o Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros e outras normas e regras aplicáveis à matéria.

Análise de Mercado

(i) Sempre avaliar se esse prestador de serviços pode gerar qualquer potencial conflito de interesse com o gestor de recursos, administrador fiduciário ou cotista dos Veículos de Investimento administrados pela HDB Gestão;

(ii) Se o valor cobrado é justo em relação ao serviço oferecido e ao valor de mercado;

(iii) Se há benefícios recebidos pela HDB Gestão e seus empregados derivados de tal contratação, ou se os benefícios são direcionados ao fundo ou ao investidor.

Processo de Pré-Seleção

Durante o processo de contratação, os empregados devem obter informações qualitativas sobre o terceiro interessado em iniciar vínculos legítimos com a HDB Gestão, a fim de permitir um melhor julgamento durante a pré-seleção. As informações a serem obtidas devem incluir:

- A data de início das atividades;

- Qualificações dos principais sócios/executivos;

- Lista de clientes (passados e atuais) e objeto da contratação;

- Busca na rede mundial de computadores sobre notícias negativas sobre o terceiro; e

- Outras informações qualitativas que possam ser relevantes para melhor avaliar o terceiro.

O terceiro deverá estar legalmente constituído, gozar de boa reputação, ter capacidade econômica, financeira e técnica compatível com o objeto do contrato e com a assunção de responsabilidades contratuais.

Cópias do cartão de registro no Cadastro Nacional da Pessoa Jurídica (CNPJ) e documentos constitutivos e/ou corporativos relevantes devem ser solicitados ao terceiro. Se necessário, devem ser solicitadas cópias das demonstrações financeiras dos últimos 3 (três) anos e referências bancárias e técnicas do terceiro.

Além disso, os seguintes aspectos devem ser considerados durante o processo de pré-seleção:

- Estrutura da empresa;

- Boa reputação (no caso de uma pessoa jurídica, a reputação dos sócios e dos principais executivos também deve ser considerada);

- Nível de satisfação de outros clientes, passados e presentes;

- Estrutura para atender o objeto da Contratação;

- Capacidade econômica e financeira;

- Código de Conduta e Ética, ou similar;

- Política Anticorrupção, ou similar;

- Política de Combate à Lavagem de Dinheiro, ou similar;

- Qualquer documento, procedimento e/ou formulário relacionado com a integridade e o cumprimento das regras; e

- Selo de Associado ou Aderente à ANBIMA, quando aplicável, ou, se não for o caso, as razões para não o obter.

O início das atividades dos empregados estará vinculado à formalização do contrato, e nenhum pagamento poderá ser feito antes da conclusão do contrato. Os acordos celebrados para formalização do contrato deverão ter os requisitos contidos no artigo 11 do Código ANBIMA de Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros.

Os empregados responsáveis pelo processo de seleção de fornecedores manterão registros atualizados dos fornecedores, eliminando aqueles sobre os quais haja qualquer dúvida relativa a má conduta, comportamento antiético, comportamento ilícito ou que possam ter uma má reputação no mercado.

Não Aplicabilidade do Processo de Pré-Seleção

A HDB Gestão poderá deixar de aplicar os procedimentos ora estabelecidos, a seu critério exclusivo, quando o terceiro não estiver relacionado ao negócio principal do gestor de recursos e tiver uma clara capacidade econômica, financeira e/ou técnica para satisfazer o objeto da contratação e para cumprir suas responsabilidades e arranjos contratuais.

Outras Disposições

Vale mencionar que, devido às regras estabelecidas na atual regulamentação e autorregulamentação, a HDB Gestão adotará medidas prévias de *due diligence* para a contratação e monitoramento de terceiros relacionados à tecnologia, sistemas e/ou infraestrutura de informação, visando à proteção de dados.

Seleção de Corretores

A HDB Gestão, com a prestação de serviços adequados que garantam a melhor execução das ordens para Veículos de Investimento e/ou carteiras administradas sob gestão, juntamente com a preservação dos interesses e, consequentemente, de seus investidores, adota um cuidadoso processo de seleção e contratação de corretores.

Esse processo é baseado na devida investigação de potenciais corretores-distribuidores de valores mobiliários para permitir que a HDB Gestão adquira um conhecimento profundo de potenciais prestadores de serviços.

Os corretores devem ser considerados como terceiros, para fins de aplicação do Processo de Pré-seleção, incluindo solicitando à corretora a qualificação PQO da B3 e o questionário padrão de *due diligence* da

Anbima.

Monitoramento

O monitoramento das atividades realizadas por terceiros para a HDB Gestão, assim como os próprios terceiros, é de responsabilidade da área que solicitou a contratação. O monitoramento deve ser contínuo durante a vigência da contratação, e o terceiro avaliado proporcionalmente ao serviço prestado, com ênfase em eventuais disparidades de tempo, qualidade e quantidade esperada.

Além disso, o monitoramento deve ser capaz de identificar preventivamente atividades que possam resultar em riscos para a HDB Gestão, e os respectivos relatórios devem ser enviados para a Equipe de *Compliance*.

No caso de qualquer fato novo ou mudança significativa, é possível reavaliar a contratação de terceiros.

É importante notar que este monitoramento se baseia no princípio dos melhores esforços, já que a HDB Gestão e seus empregados não podem estar presentes no dia a dia de terceiros contratados a todo tempo.

Manutenção de Documentos

Todos os manuais, relatórios, atas e outros documentos relacionados a essa seleção de terceiros e à Política de Contratação e Monitoramento serão mantidos em arquivos físicos ou armazenados digitalmente no escritório da HDB Gestão por um mínimo de cinco (05) anos.

VIOLAÇÃO

A violação desta Política pode resultar em aplicação pelo Diretor de *Compliance* das sanções que julgar apropriadas, incluindo, entre outras coisas, uma carta de censura, suspensão ou rescisão do contrato de trabalho do infrator . A HDB Gestão se reserva o direito de notificar as autoridades competentes de aplicação da lei sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade.

DISPOSIÇÕES GERAIS

Esta Política está disponível no website da HDB Gestão, de acordo com o Artigo 16, III da Resolução CVM 21.

PRAZO E ATUALIZAÇÃO

Este Manual será revisado anualmente pela HDB Gestão e será alterado na medida em que houver a necessidade de atualizar seu

conteúdo. PRAZO E ATUALIZAÇÃO

DOCUMENT – REVISIONS

REVISION #	PREPARED BY	DATE	REVIEWED BY	DATE	AMENDMENT DETAILS
001	Compliance Brazil	04.2024	Compliance Houston	04.2024	Final