2023

BRAVOS GESTÃO DE RECURSOS LTDA.

Manual de Segregação de Atividades e Segurança da Informação

MANUAL DE SEGREGAÇÃO DE ATIVIDADES E SEGURANÇA DA INFORMAÇÃO

1. Objetivo e Atividades da Gestora

Este Manual de Segregação de Atividades e Segurança da Informação ("Manual") da Bravos Gestão de Recursos Ltda. ("Gestor") foi elaborado de acordo com os artigos 27 e 28 da Resolução CVM 21, de 25 de fevereiro de 2021 ("Resolução CVM 21") e tem como finalidade: (i) garantir a segregação física de instalações entre o Departamento Técnico (também referido como "Gestão") e as áreas responsáveis por *Compliance*, Riscos e PLDFT e Controladoria (juntas, o "*BackOffice*") do Gestor; (ii) assegurar o bom uso de instalações, equipamentos e informações comuns; (iii) preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas; e (iv) restringir o acesso a arquivos e permitir a identificação das pessoas que tenham acesso a informações confidenciais.

Adicionalmente, o Manual também abrange as questões relacionadas à Segurança da Informação, que contarão com prestadores de serviço especializados visando garantir a eficiência e segurança compatíveis com as necessidades do Gestor, de suas pessoas Colaboradoras, investidores e demais *stakeholders*, bem como a responsabilização dos envolvidos em caso de violação (vazamentos).

Não exercício das atividades de Distribuição e Intermediação:

O Gestor atua no setor de *private Equity*, adotando fundos de investimentos em participações ("FIPs") como veículos para investimentos de seus clientes/investidores. Considerando que não serão performadas atividades de distribuição de cotas dos fundos de investimento sob gestão e, tampouco, de intermediação, este Manual terá relevância reduzida em relação aos demais e em relação aos demais players do mercado de capitais. Sem prejuízo, suas disposições serão aplicáveis a todos os sócios(as), empregados(as), Diretores(as), funcionários(as) e estagiários(as) do Gestor ("Colaboradores").

Ausência de Conflito entre Gestão e *BackOffice*:

A definição da política de investimento do Gestor consta dos acordos assinados entre o Gestor e cada um dos seus investidores, bem como dos regulamentos dos FIPs sob gestão. Neste sentido, o Gestor não identificou potenciais conflitos de interesses entre o Departamento Técnico e o *BackOffice,* (que exerce atividades da mesma natureza também para veículos de investimento estrangeiros), e/ou em relação ao gerenciamento dos recursos financeiros próprios do Gestor (que são aplicados apenas em fundos de investimentos de terceiros ou em Certificados de Depósitos Bancários emitidos por instituições financeiras).

2. Estrutura

Considerando a estrutura do Gestor, foram desenvolvidas regras aplicáveis à (i) segregação física entre o Departamento Técnico e o *BackOffice*; (ii) *Chinese Wall*; e (iii) à segurança da informação do Gestor.

No que se refere a ao item (iii) acima, os prestadores de serviço de tecnologia da informação são contratados pelo *BackOffice* e são responsáveis pela implantação e racionalização de processos, manutenção dos sistemas de informática, segurança da informação com controle de acesso dos usuários e *backup* de dados.

3. Segregação física

O acesso à área utilizada pela equipe especializada na gestão de carteiras de valores mobiliários será permitido às pessoas Colaboradoras autorizadas. Referida área ocupa sala completamente apartada, comunicando-se apenas com serviços auxiliares à atividade de gestão de carteiras de valores mobiliários, de forma a manter-se fisicamente segregada de quaisquer áreas do Gestor que venham a ser responsáveis por outras atividades relacionadas ao mercado de capitais.

É limitado o acesso às instalações físicas da área de gestão de carteiras de valores mobiliários por pessoas que não sejam pessoas Colaboradoras envolvidos na atividade de gestão de carteiras de valores mobiliários.

4. *Chinese Wall*

Tem como finalidade estabelecer uma barreira de comunicação entre diferentes indivíduos ou setores de uma mesma entidade, visando assegurar o cumprimento das normas que exigem a segregação entre a atividade de administração de carteiras de valores mobiliários e outras atividades relacionadas ao mercado de capitais, bem como a segregação entre ativos financeiros próprios do Gestor e os ativos financeiros de terceiros.

Via de regra, as restrições de acesso às informações e aos documentos contidos na rede de computadores e sistemas do Gestor respeitam o organograma funcional. Exceções, no entanto, poderão ser avaliadas pela Diretoria de *Compliance* e Riscos conforme solicitação fundamentada e avaliação de necessidade.

5. Confidencialidade, Sigilo e Segurança da Informação

Informações Confidenciais:

No exercício de suas atividades, as pessoas Colaboradoras poderão ter acesso a informações de clientes do Gestor, bem como de terceiros, que não sejam de conhecimento do público em geral e que, portanto, possam ser consideradas confidenciais ("Informações Confidenciais" ou, no singular, "Informação Confidencial"). É terminantemente proibida a divulgação de qualquer Informação Confidencial para terceiros, para benefício próprio ou de terceiro (*tipping*), ou mesmo que não haja intenção de beneficiar ninguém. A obrigação de confidencialidade se aplica mesmo após o desligamento da pessoa Colaboradora.

O Gestor e as pessoas Colaboradoras possuem o dever legal e profissional de manter o sigilo quanto às Informações Confidenciais de seus clientes/invetidores, de modo que pedidos, tentativas ou ações visando a quebra do sigilo deverão ser imediatamente comunicados à Diretoria de *Compliance* e Riscos, para que decida quanto à sua regularidade e necessidade.

Informações Sigilosas:

Informações Sigilosas, além das Informações Confidenciais, são aquelas que, caso venham à tona, podem resultar em perda do nível de segurança do Gestor.

Perda, mau uso, modificação ou acesso não autorizado às Informações Sigilosas podem afetar adversamente a privacidade de um indivíduo, desfazer negócios, macular a imagem do Gestor e a continuidade de seus negócios.

O Gestor tem a responsabilidade legal de prezar pelo sigilo de seus clientes e, portanto, informações relativas aos clientes e entidades investidas por fundos de investimento geridos pelo Gestor jamais poderão ser enviadas a terceiros, com exceção das solicitações dos órgãos públicos,

dos órgãos reguladores e do Poder Judiciário e, mesmo nessas hipóteses, nos estritos limites das ordens recebidas.

Segurança da Informação:

As medidas de segurança da informação têm por finalidade a proteção contra ameaças, de modo a garantir a continuidade dos negócios, minimizar riscos e maximizar os retornos aos investidores.

Tais medidas estão sob a responsabilidade dos serviços de tecnologia da informação – terceirizada para garantia de qualidade e sob responsabilidade da Controladoria, conforme será descrito nos próximos itens deste Manual -, e devem ser observadas por todos as pessoas Colaboradoras:

Causam situações de risco à Segurança da Informação:

(i) Acessar a sites não relacionados às atividades do Gestor;
(ii) Utilizar mídias ("pen-drives", CDs, entre outras) para armazenamento de arquivos digitais, com exceção das disponibilizadas pelo Gestor;
(iii) Acessar ou salvar informações sensíveis e Informações Confidenciais em pastas virtuais de acesso público;
(iv) Salvar arquivos pessoais na rede de computadores institucional;
(v) Utilizar mídias para transporte de informações não criptografadas;
(vi) Dividir senhas.

Mais informações poderão ser encontradas no Anexo I do presente Manual, que contém algumas regras referentes ao Gerenciamento e Segurança de Informações Confidenciais.

6. Reporte, Penalidades e Responsabilidade

É dever de toda pessoa Colaboradora informar à Diretoria de *Compliance* e Riscos sobre violações ou possíveis ou suspeitas violações das disposições referentes à Segregação Física contidas neste Manual, sendo certo que o descumprimento de qualquer regra estabelecida neste Manual implicará, a critério da Diretoria de *Compliance* e Riscos, as seguintes penalidades, a depender da gravidade do descumprimento e de eventual reincidência: (i) advertência por escrito; ou (ii) desligamento.

Qualquer pessoa Colaboradora que acredite ter violado este Manual ou tenha conhecimento ou suspeita de violação deverá notificar o fato direta e imediatamente à Diretoria de *Compliance* e Riscos, sendo que eventual ação disciplinar levará o reporte em consideração. Ainda, poderão ser tomadas ações disciplinares contra pessoa Colaboradora que (i) autorize, coordene ou participe de violações a esta Política; (ii) possuindo informação ou suspeita de violações, deixe de reportá-las; (iii) deixe de reportar violações ocorridas que, pelo seu dever de ofício, deveria ter conhecimento ou suspeita; e/ou (iv) promova retaliações, direta ou indiretamente, ou encoraje outros a fazê-lo.

No que se refere à Segurança da Informação, a responsabilidade pela contratação e fiscalização dos serviços de prestados será de responsabilidade da Controladoria, que avaliará os terceiros com potencial de contratação nos termos do Manual de *Compliance* e demais normas internas e fará o acompanhamento e avaliação qualitativa dos serviços prestados

Acompanhamento:

Caso haja ocorrência, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual, caberá à Diretoria de *Compliance* e Riscos utilizar os registros eletrônicos disponíveis para verificar a conduta das pessoas Colaboradoras.

A Diretoria de *Compliance* e Riscos terá acesso a todo conteúdo que está na rede de computadores do Gestor e poderá acessar tal conteúdo caso haja necessidade. A confidencialidade das informações será respeitada e seu conteúdo será disponibilizado somente para fins legais[1], garantindo, assim, verificação dos responsáveis por eventuais vazamentos.

7. Diretor(a) Responsável

Abaixo apresentamos informações cadastrais do(a) Diretor(a) de *Compliance* e Riscos responsável por *Compliance*, Gestão de Riscos e PLDFT do Gestor:

Nome	Emir Josafaf Calvo Correia
E-mail	*compliance@bravosgestao.com.br*
Telefone	(21) 3235-0770 ou (11) 3074-0920

Por fim, o Gestor atesta que o(a) Diretor(a) de *Compliance* e Riscos não está subordinado às demais áreas de atuação, incluindo a gestão de recursos ou a área comercial.

8. Atualização

Este Manual será submetido à revisão anual ou em períodos inferiores a este, sempre que o(a) Diretor(a) de *Compliance* e Riscos considerar necessário, com o intuito de preservar as condições de segurança para o Gestor.

Versão	Data	Responsabilidade
1	Dezembro de 2020	Suelen Marinho de Souza
2	Maio de 2021	Márcia Regina Brambilla
3	Junho de 2022	Emir Josafaf Calvo Correia
4	Maio de 2023	Emir Josafaf Calvo Correia

[1] Da mesma forma, as mensagens de correio eletrônico profissional das pessoas Colaboradoras poderão ser interceptadas e abertas para ter a regularidade de seu conteúdo verificada, computadores poderão ser auditados e conversas telefônicas poderão ser gravadas e escutadas sem que isto represente invasão da privacidade das pessoas Colaboradoras, já que se tratam de ferramentas de trabalho disponibilizadas pelo Gestor, o que poderá ocorrer em qualquer momento que o(a) Diretor(a) de *Compliance* e Riscos julgue necessário.

ANEXO I - SISTEMA DE GERENCIAMENTO E SEGURANÇA DE INFORMAÇÕES

O Gestor considera o gerenciamento das informações um assunto de âmbito estratégico, uma vez que as decisões que permeiam a gestão de seus ativos dependem da confiabilidade, segurança e acessibilidade ao sistema de gerenciamento de informações.

Para atingir estes objetivos, o Gestor estabeleceu regras de *Compliance* e de gestão de segurança em TI.

Gerenciamento de Informações Confidenciais

Quanto aos parâmetros de C*ompliance*, o Gestor, quando sistemicamente permitido, define os perfis de acesso de cada usuário da rede interna de computadores de forma que as Informações Confidenciais fiquem acessíveis somente por determinadas pessoas do Gestor, autorizadas pela Diretoria de *Compliance* e Riscos. Ficam preservadas as informações de clientes e ao mesmo tempo evitam-se problemas relacionados a conflitos de interesses ou uso indevido de Informações Confidenciais.

Além disso, o controle de tráfego de dados entre as pessoas Colaboradoras é realizado por meio de sistemas de "*firewall*" e controle de acessos à rede de computadores, que são responsáveis pela proteção de Informações Confidenciais. Dessa forma, controla-se quem efetivamente acessou determinados dados e/ou sistemas e ficam impedidos acessos não autorizados.

Assim, foram definidos níveis de acesso para os membros do Comitê de *Compliance* e Riscos, do Departamento Técnico e do *BackOffice*.

No que se refere ao gerenciamento de riscos referentes à segurança da informação, a Bravos atuará por meio de rotinas elaboradas por prestadores de serviço especializados para assegurar um ambiente resguardado de qualquer tipo de risco para as informações e para a rede interna de computadores, evitando que a qualidade da gestão seja afetada por contingências.

Estrutura de Tecnologia de Informação e Hardware:

Em complemento às informações contidas no item acima, o Gestor terá uma rede integrada de computadores, revisados quanto à capacidade, segurança e nível de atualização de seus componentes, com o suporte técnico de empresa terceirizada contratada. Além disso, serão adotados procedimentos contínuos relacionados aos *softwares* de antivírus, responsáveis por proteger, durante 24 (vinte e quatro) horas por dia, sem interrupção, a rede interna de computadores da Bravos e o computador de cada colaborador.

Ainda, com relação aos e-mails, o Gestor utilizará equipamentos atualizados e seu servidor de e-mails será hospedado junto a Microsoft, através do *Exchange Online*, o que garantirá alta disponibilidade e segurança e viabilizará o trabalho remoto e via computadores reserva, se e quando necessário, sem prejuízo da manutenção de registros que irá viabilizar a realização de auditorias e inspeções nos termos dos manuais e políticas da gestora.

No que tange aos *ids* das pessoas Colaboradoras e aos computadores, sua administração ocorrerá de forma centralizada através de servidor, onde (i) usuários e suas atividades podem ser monitorados; (ii) o particionamento das pastas é viabilizado; e (iii) os perfis de acesso são configurados conforme as prerrogativas e necessidades inerentes aos cargos das pessoas Colaboradoras.

Adicionalmente, com relação à estrutura de telefonia, o Gestor terá PABX com canais na sala de gestão, linha exclusiva para uso de fax e linhas móveis corporativas (para uso das pessoas Colaboradores sempre que necessário) como meios de comunicação.

Por fim, todos as pessoas Colaboradoras do Gestor terão acesso a atendimento relacionado aos sistemas de tecnologia da informação por diferentes canais, podendo optar pelo atendimento via telefone central, via celular dos colaboradores e, ainda, por meio de visitas periódicas e/ou emergenciais.