BALUARTE CAPITAL GESTÃO DE RECURSOS LTDA.

POLÍTICA DE *COMPLIANCE* E CONTROLES INTERNOS DA BALUARTE CAPITAL

Data-Base: 09 de abril de 2024

SUMÁRIO

1. POLÍTICA DE *COMPLIANCE* E CONTROLES INTERNOS

1.1. INTRODUÇÃO E EMBASAMENTO LEGAL

A Baluarte Capital, representada pelo Diretor de *Compliance*, fiscalizará continuamente os Colaboradores, quanto ao cumprimento das Políticas Internas previstas neste documento.

Observada a competência do Comitê de Ética, o Diretor de *Compliance*, entre outros assuntos, é responsável por criar e monitorar as regras com relação aos controles internos, procedimentos operacionais, políticas de prevenção e combate à lavagem de dinheiro e adequação da Baluarte Capital às leis e regulamentações aplicáveis.

Esta política também é utilizada para estimular a constante atualização e o treinamento dos Colaboradores de forma a manter a excelência na prestação dos serviços aos clientes. Serve ainda para monitorar possíveis erros operacionais, conflitos de interesses e assegurar a adesão às demais políticas da Baluarte Capital, todas divulgadas no endereço eletrônico disponibilizadas em via impressa e digitalizada a todos os Colaboradores.

O *compliance* interno da Baluarte Capital envolve as seguintes atividades:

i. fiscalização periódica de rotinas, regras e procedimentos previstos nas Políticas Internas, a fim de identificar eventuais violações;

ii. manutenção de canal para recebimento de dúvidas, esclarecimentos, denúncias ou reclamações, a serem dirigidas ao Diretor de Compliance, por meio de correio eletrônico enviado ao seguinte endereço: andre@baluartecapital.com. Nenhum Colaborador será advertido, sofrerá retaliação e/ou será penalizado por realizar denúncias de boa-fé ao Diretor de Compliance, ainda que posteriormente seja afastada após apuração da ilicitude da conduta denunciada;

iii. aplicação de penalidades aos Colaboradores que violem as Políticas Internas, as quais poderão envolver ações disciplinares, incluindo advertência, desligamento do quadro societário da Baluarte Capital, término do vínculo empregatício ou rescisão do

contrato de prestação de serviços ou do contrato que o vincula à Baluarte Capital, conforme aplicável, sem prejuízo de eventuais medidas administrativas e/ou legais cabíveis;

iv. coordenação de interações da Baluarte Capital com seus reguladores e órgãos de autorregulação, bem como coordenação com as demais áreas e departamentos para fortalecer o ambiente de controle geral da Baluarte Capital;

v. solicitar, sempre que necessário, o apoio de consultores externos para análise de questões mais complexas envolvendo o compliance interno da Baluarte Capital; e

vi. atualização periódica das Políticas Internas, a fim de refletir mudanças legislativas, regulamentares, de autorregulação e melhores práticas do mercado.

Este Capítulo traz disposições gerais sobre o compliance interno da Baluarte Capital. No caso de conflito entre as disposições gerais previstas neste Capítulo e as disposições de Políticas Internas específicas, prevalecerão as disposições das Políticas Internas específicas.

EMBASAMENTO LEGAL

Para a elaboração da presente política, foram utilizados os mais relevantes instrumentos normativos, sejam nacionais ou internacionais, que versam sobre a responsabilidade e obrigações referentes à estrutura de Compliance e de Controles Internos, podendo se citar:

- Lei nº 4.728/1965;
- Lei nº 6.385/1976;
- Lei nº 10.303/2001;
- Resolução da Comissão de Valores Mobiliários nº 135/2022;
- Resolução da Comissão de Valores Mobiliários nº 21/2021;
- Resolução da Comissão de Valores Mobiliários nº 35/2021.

1.2 ABRANGÊNCIA

A presente Política de Compliance Controles Internos se aplicará indistintamente a todos colaboradores e funcionários da Baluarte Capital, devendo ser cumprido de forma obrigatória.

1.3 POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E CIBERSEGURANÇA

As atividades de administração e gestão de carteiras compreendem o acesso a Informações Confidenciais de propriedade de seus clientes. A Baluarte Capital entende a seriedade e o nível de confiança depositados pelos clientes na Baluarte Capital e, portanto, trata a segurança da informação com elevada seriedade.

Em razão do grau de zelo pela segurança e integridade das Informações Confidenciais, a Baluarte Capital instituiu a Política de Segurança de informação e Cibersegurança, onde é prevista as diretrizes específicas na correta condução e tratamento das Informações Confidenciais, a qual é de aceite obrigatório por todos os Colaboradores da Baluarte Capital.

Conforme disposto no artigo 24 da Resolução 21 da Comissão de Valores Mobiliários, todos os arquivos da Baluarte Capital são armazenados em servidores cujas empresas possuem reputação profissional ilibada nos respectivos campos de atuação.

Todos os acessos aos sistemas utilizados pelos Colaboradores são protegidos por senhas e quaisquer documentos físicos que contenham Informações Confidenciais sobre o patrimônio dos clientes possuem codificação no lugar dos nomes completos.

Adicionalmente, a Baluarte Capital garante a realização de testes regulares de segurança nos sistemas de informação, especialmente nos mantidos em meio eletrônico.

O livre acesso às instalações físicas da Baluarte Capital é restrito aos Colaboradores, sendo o ingresso nas instalações físicas da Baluarte Capital por clientes assessores técnicos e prestadores de serviços, limitado às áreas em que não são realizadas as atividades de administração de carteiras de valores mobiliários (como, por exemplo, as salas de reunião).

1.4 TREINAMENTOS E CERTIFICAÇÕES

A Baluarte Capital acredita que o aprendizado contínuo dos Colaboradores eleva o nível de conhecimento da equipe e agrega valor à Baluarte Capital.

Portanto, a Baluarte Capital incentiva que todos os colaboradores busquem aprimorar seus conhecimentos, através de ações e programas de aperfeiçoamento.

Este aprimoramento pode ser feito através de treinamentos internos e externos, cursos externos (graduação, pós-graduação, especialização e/ou capacitação) e/ou certificações exigidas pelas regulamentações vigentes.

Não obstante, os Colaboradores receberão treinamentos internos apropriados relativos às disposições das Políticas Internas, os quais compreenderão, inclusive, mas não se limitando a, conceitos relativos à segurança da informação, negociação por detentores de informação privilegiada e segregação de informação.

Os treinamentos serão realizados pelo menos 1 (uma) vez por ano, em data a ser determinada pela Baluarte Capital, sob a supervisão do Diretor de Compliance, sendo que a presença de todos os Colaboradores é obrigatória. Cada Colaborador assinará uma declaração de que participou do treinamento.

1.5 PLANO DE CONTINGÊNCIA

Em razão da natureza das atividades de gestão de recursos desenvolvidas pela Baluarte Capital, a sociedade está sujeita a extensa legislação, regulamentação e autorregulação no mercado brasileiro. A fim de atender integralmente a essas exigências, bem como adaptar suas atividades às melhores práticas de mercado, a Baluarte Capital adota a presente política que descreve os Planos de Contingência para a Continuidade de Negócios ("PCCN"), sob responsabilidade direta do Diretor de Compliance.

O PCCN visa garantir a continuidade dos negócios da Baluarte Capital na ocorrência de eventos de caso fortuito ou força maior que possam afetar sua infraestrutura física ou tecnológica ("Evento Disruptivo").

O PCCN encontra-se descrito abaixo e deverá ser revisado e atualizado anualmente pelo Diretor de Compliance, visando assegurar a continuidade de transações e negócios durante situações adversas, de emergência ou catástrofes.

1.5.1 LOCAL DE TRABALHO E COLABORADORES

Em caso de um evento que impossibilite o acesso de Colaboradores ao escritório da Baluarte Capital, estes devem retornar a suas respectivas residências, a fim de desenvolver suas funções a partir do acesso remoto à rede da Baluarte Capital (mediante uso de suas credenciais para liberação do acesso) e aguardar instruções do Diretor de Compliance. A comunicação será realizada por meio de ligação telefônica ou e-mail.
Caso o escritório permaneça fechado por mais de 24 (vinte e quatro) horas em um dia útil, os Colaboradores devem manter as atividades à distância, salvo na hipótese de o Diretor de Compliance optar por alocar a equipe de trabalho em um local de apoio, a ser definido por ele.

O sistema de tecnologia da Baluarte Capital possui a opção de acesso remoto, permitindo aos Colaboradores o exercício normal de suas atividades sem a presença física nas dependências da sociedade, conforme subitem 6.4.4.

1.5.2 COMUNICAÇÃO

Como prevenção à hipótese de interrupção de qualquer meio de comunicação utilizado pela Baluarte Capital, todos os Colaboradores são orientados a manter em suas residências uma cópia atualizada de ao menos 3 (três) meios de comunicação para contato com todos os demais colaboradores, tais como 2 (dois) números de telefone e e-mail. Essa lista será providenciada pelo Diretor de Compliance e conterá os nomes e 3 (três) formas de contato de todos os Colaboradores. Caso ocorra qualquer Evento Disruptivo, cada Colaborador será contatado e informado acerca da ocorrência nos 3 (três) meios de comunicação disponíveis.

Adicionalmente, assim que possível, todos os clientes serão notificados (via e-mail, correspondência ou telefonema) pela Baluarte Capital sobre a ocorrência do Evento Disruptivo, as formas alternativas de contato e prazos de solução do problema pela Baluarte Capital. O Diretor de Compliance será responsável por realizar essa comunicação.

1.5.3 PROTEÇÃO DE ARQUIVOS

Todos os arquivos e registros da Baluarte Capital terão cópias de segurança em nuvem, no One Drive. Essa empresa possui equipe profissional dedicada à segurança da informação e utilizam as melhores ferramentas/práticas de engenharia disponíveis para manter seguros e atualizados todos os arquivos (dentre as ferramentas utilizadas para esse

fim, figuram a adoção do padrão de criptografia Advanced Encryption Standard (AES) e Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para proteger os dados em trânsito entre os aplicativos do One Drive e servidores). Além de manter os arquivos e registros em nuvem, a Baluarte Capital faz cópias em hard drives locais. Dessa forma, qualquer problema técnico em via física do documento ou equipamento eletrônico não obstará o acesso ao conteúdo de qualquer arquivo da sociedade.

1.5.4 ACESSO REMOTO AOS SISTEMAS DA BALUARTE CAPITAL

Os Colaboradores poderão exercer suas funções de qualquer computador com acesso à rede mundial de computadores. O acesso remoto aos sistemas essenciais da Baluarte Capital estará disponível, com logins e senhas individuais para todos os Colaboradores. Os Colaboradores devem configurar seus computadores particulares para terem acesso aos arquivos nos sistemas da Baluarte Capital. O e-mail profissional poderá ser acessado via internet por todos os Colaboradores.

1.5.5 QUEDA DE ENERGIA – NO BREAKS

Todos os acessos a sistemas digitais da Baluarte Capital são realizados por meio de desktop e/ou dispositivos móveis, com autossuficiência mínima de até 1 (uma) hora de funcionamento sem fonte de energia. Todos os Colaboradores da Baluarte Capital são orientados a manter seus dispositivos móveis com armazenamento completo de bateria.

Em caso de quedas repentinas e abruptas de energia, os Colaboradores devem reduzir ao máximo a execução de atividades que necessitam de energia elétrica, promovendo simultaneamente a finalização de tarefas necessárias e armazenagem de documentos em execução.

1.5.6 IMPLEMENTAÇÃO DE PROCEDIMENTOS EMERGENCIAIS

A tabela abaixo descreve os eventos, procedimentos e divisão de atribuições a serem adotados em casos de emergência:

Evento	Procedimento	Quem acionar
- Prédio inacessível - Evacuação	- Ativação da estrutura de home-office: uso de laptops e celulares corporativos - Acesso remoto à rede local (se disponível) e acesso direto a arquivos salvos na nuvem - Redirecionamento das ligações para os respectivos celulares	Diretor de *Compliance* e/ou Diretor de Gestão de Riscos
- Queda de energia prolongada	- Utilização dos laptops e celulares no próprio escritório - Principais atividades disponíveis no servidor em nuvem - Backup de todas as atividades disponíveis assim que energia for restabelecida	Diretor de *Compliance* e/ou Diretor de Gestão de Riscos
- Falha na rede de internet	- Duplicidade de Link com servidores diferentes (Mundivox e Vivo) - Em caso de queda simultânea dos 2 (dois) links, - será utilizada a internet dos celulares corporativos e/ou *home-offices*	Diretor de *Compliance* e/ou Diretor de Gestão de Riscos
- Interrupção por falha no servidor	- Duplicidade de Servidores compatíveis - Transferência dos back-ups da unidade inacessível para a unidade disponível	Diretor de *Compliance* e/ou Diretor de Gestão de Riscos

2. ATUALIZAÇÕES

Versão	Motivo da Alteração	Data de Aprovação	Autor
Última Versão	Revisão Periódica	26/10/2022	Diretor de Compliance
Penúltima Versão	Revisão Periódica	22/06/2023	Diretor de Compliance
Versão Atualizada	Revisão Periódica	09/04/2024	Diretor de Compliance