MANUAL DE COMPLIANCE E CONTROLES INTERNOS

Citrino Gestão de Recursos Ltda.

Versão 1.2 – 13 de agosto de 2025.

Introdução

A Citrino Gestão de Recursos Ltda. ("Citrino" ou "Gestora") é uma sociedade limitada autorizada pela Comissão de Valores Mobiliários ("CVM") a prestar o serviço de administração de carteira de títulos e valores mobiliários na carteira gestor de recursos.

O Manual de Controles Internos e Compliance ("Manual") da Citrino tem por objetivo garantir o atendimento às normas, políticas e regulamentações vigentes, por meio de controles internos adequados e aplica-se a todos sócios, administradores, diretores, funcionários, estagiários ou consultores da Citrino ("Colaboradores") no desempenho de suas atividades.

Nesse sentido, o Manual contempla os seguintes documentos internos da Citrino: (i) Política de treinamento; (ii) Política de segurança e sigilo das informações; (iii) Política de segregação de atividades; (iv) Plano de continuidade de negócios; e (v) Política de segurança cibernética.

No exercício de suas atividades os Colaboradores devem observar também as demais Políticas Internas e normas da Citrino, principalmente: (i) Código de Conduta; (ii) Manual de PLD/FTP e Anticorrupção; (iii) Política de escala de risco de FIFs, suitability e gestão de patrimônio; (iv) Política de Exercício de Direito de Voto; (v) Política de Rateio e Divisão de Ordens; (vi) Manual de Gestão de Riscos; e (vii) Política de Proteção de dados e privacidade.

Estrutura

A área de Controles Internos e Compliance da Citrino é de responsabilidade do Diretor de Compliance, que no exercício de sua função possui independência para:

(i) planejar, definir e implementar o programa de compliance da Citrino;

(ii) analisar possíveis violações às políticas, regras e procedimentos da Citrino ou às leis e regulações aplicáveis às atividades da Gestora;

(iii) determinar auditorias, investigações internas e, se necessário, medidas corretivas;

(iv) prevenir e disciplinar violações de Colaboradores às políticas;

(v) analisar e decidir sobre conflitos de interesse em geral.

O Diretor de Compliance, nos termos do artigo 4º, paragráfo 3º, da Resolução CVM nº 21 (i) exerce suas funções com independência em relação às demais áreas da Citrino; e (ii) não atua em funções relacionadas à administração de carteiras de valores mobiliários, à intermediação e distribuição ou à consultoria de valores mobiliários, ou em qualquer atividade que limite a sua independência, na Citrino ou fora dela.

Comitê de Compliance

A Citrino possui um comitê de Compliance, que será constituído pelo Diretor de Compliance e convidados, com no mínimo dois Colaboradores. O comitê reunir-se-á ordinariamente nos meses pares de cada ano civil. Se necessário, a diretoria de Compliance solicitará um comitê extraordinário para matérias específicas.

O comitê de Compliance é responsável por avaliar, revisar e aprovar as políticas, manuais e procedimentos de controles internos e compliance. Além disso, por iniciativa da diretoria de Compliance, o Comitê também poderá atuar em conjunto com esta para resolver conflitos de interesse, oferecer orientações ou esclarecimentos e tratar de quaisquer outros assuntos que lhe sejam submetidos.Todos os comitês serão registrados em ata assinada pelos presentes e salva na rede da Gestora.

I. POLÍTICA DE TREINAMENTO

A política de treinamento tem como objetivo estabelecer os procedimentos de treinamento dos Colaboradores. Os treinamentos têm foco na capacitação e esclarecimento das regras, procedimentos e controles internos de todas as políticas internas da Citrino.

Os Colaboradores, inclusive sócios e administradores da Citrino, deverão obrigatoriamente participar do treinamento periódico. O treinamento periódico será realizado, no mínimo, uma vez por ano e incluirá obrigatoriamente as matérias de PLD/FTP e conflitos de interesses.

Novos colaboradores receberão o treinamento de forma individual, visando também a apresentação das atividades desenvolvidas e estrutura da Citrino.

A diretoria de Compliance é responsável pelo controle e agendamento dos treinamentos. Após o evento os Colaboradores assinarão o Termo de compromisso e confidencialidade do ano corrente..

II. POLÍTICA DE SEGURANÇA E SIGILO DAS INFORMAÇÕES

A política de segurança e sigilo das informações da Citrino tem por objetivo assegurar o controle de informações não públicas e garantir a confidencialidade das informações que os seus Colaboradores têm acesso no exercício de suas atividades.

A confidencialidade é um princípio fundamental para a Citrino e aplica-se a qualquer informação não pública obtida na condução de negócios por seus Colaboradores.

Os Colaboradores devem observar as vedações e regras determinadas abaixo durante a vigência do seu relacionamento profissional com a Citrino e após seu término:

Vedações

(i) Transmitir, copiar ou fazer ou download de imagens ou vídeos de conteúdo pornográfico, racista ou que remeta a qualquer forma de preconceito.

(ii) Transmitir informações não públicas a terceiros.

(iii) Utilizar material, marca e logotipos da Citrino para assuntos não corporativos.

(iv) Transmitir, copiar, postar os arquivos utilizados, gerados ou disponíveis na rede da Citrino, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais e de propriedade da Gestora. Tal proibição não se aplica quando as cópias ou a

impressão dos arquivos forem em prol e do desenvolvimento dos negócios e dos interesses da Citrino.

Regras de Conduta

(i) Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

(ii) A estrutura física e eletrônica da Citrino deve ser utilizada de forma ética e profissional, visando somente as atividades da Gestora.

(iii) Computadores e telefones, entre outros dispositivos, são considerados ferramentas de trabalho e não devem ser utilizados para assuntos particulares.

(iv) A senha do acesso individual é confidencial e ela não deve ser distribuída ou comunicada a terceiros.

(v) Toda a comunicação eletrônica referente às atividades da Gestora deve ser realizada através do e-mail profissional ou outras ferramentas disponibilizadas pela Citrino.

(vi) Os Colaboradores devem guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, até sua divulgação ao mercado, e zelar para que subordinados também o façam.

(vii) Os Colaboradores devem preservar a confidencialidade de informações relativas a operações em andamento e informações recebidas de entidades/pessoas cuja publicidade ou posição possa influenciar o mercado.

(viii) Na suspeita ou identificação de uma falha no controle de acesso e disponibilidade de informações, o Colaborador deve reportar imediatamente à diretoria de Compliance.

A Citrino se reserva no direito de gravar ligações telefônicas e monitorar qualquer outro meio disponibilizado pela Gestora para a atividade profissional do Colaborador.

Todo Colaborador assinará um Termo de Compromisso, que reforça da obrigação de observância da política de segurança e sigilo da informação da Gestora. Por esse termo, cada Colaborador declara ciência da existência da referida política, assim como das regras e princípios seguidos pela Citrino.

III. POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES

A política de segregação de atividades da Citrino tem por objetivo estabelecer os procedimentos e regras para a segregação física entre a área responsável pela administração de valores mobiliários das demais atividades que, eventualmente, possam gerar conflitos de interesse.

O exercício da administração de carteiras de valores mobiliários é desenvolvido pela Citrino através dos serviços de gestão de patrimônio financeiro, gestão de recursos de terceiros e gestão-distribuição.

Segregação física

A sala de operações, área destinada às atividades funcionais, é fisicamente segregada das áreas comuns da Citrino, como por exemplo, recepção e salas de reunião, e acessada exclusivamente pelos Colaboradores.

O acesso de terceiros à sala de operações deve ser realizado com acompanhamento de Colaboradores e aviso prévio a diretoria de Compliance.

Destaca-se que a segregação física não é mandatória entre a área responsável pela gestão e a área responsável pela distribuição de cotas de classes de investimentos onde a Citrino, cumulativamente, é gestor de recursos.

Segregação eletrônica

O acesso aos diretórios é configurado de acordo com a área de atuação e senioridade do Colaborador.

Apesar dessa segregação, para permitir que as atividades internas aconteçam de modo eficiente, certas informações serão compartilhadas na base da necessidade dos comitês da Citrino, sendo que os participantes se responsabilizam pelo sigilo das informações.

Considerações

Na ampliação do escopo das atividades da Citrino, a política de segregação de atividades será atualizada para assegurar a segregação funcional das áreas.

A diretoria de Compliance deve registrar visitas à sala de operações que considerar pertinente e falhas na segregação de atividades na ata do comitê de Compliance.

IV. PLANO DE CONTINUIDADE DE NEGÓCIOS

O plano de continuidade de negócios da Citrino tem por objetivo implementar os planos de contingência para assegurar a normalização das atividades da Citrino, bem como a integridade das informações processadas em sistemas sob sua responsabilidade e interfaces com sistemas de terceiros dentro de um intervalo adequado.

Riscos potenciais e planos de contingência

A diretoria de Compliance e a equipe de TI da Citrino analisou como riscos potenciais e definiu planos de contingências, com designação das equipes responsáveis pela operacionalização, as conjunturas abaixo:

(i) Queda de energia: caso haja falta de energia na região, o gerador do condomínio entra em atividade em até 90 (noventa) segundos, durante esse período, internamente, a Citrino conta com dois nobreaks em seu parque tecnológico que atende as todas as máquinas e servidores.

(ii) Falhas no provedor de internet: a Citrino possui dois links de internet e caso haja queda do link principal, o link redundante e dedicado está trabalhando em paralelo. A equipe de TI é responsável pelo monitoramento dos provedores e operacionalização de um plano de ação.

(iii) Contingência com servidor de e-mail: as contas de e-mail da Citrino são hospedadas em ambiente cloud, e pode ser acessada por webmail ou celular através de um ponto de internet.

(iv) Contingência com a telefonia: a Citrino possui métodos alternativos de comunicação (Whatsapp, Microsoft Teams, etc) e além disso, conta com números de celulares independentes para uso em caso de falha do PABX. O plano de ação é de responsabilidade da diretoria de Compliance.

(v) Falhas em computadores: a Citrino possui computadores backups caso haja a necessidade de substituição do equipamento para algum colaborador. A manutenção do parque tecnológico e o plano de ação é de responsabilidade da equipe de TI.

(vi) Evacuação das instalações: todos os colaboradores da Citrino são treinados para a evacuação das instalações físicas.

(vii) Site de contingência: a Citrino possui backup em cloud dos servidores e o VPN da Gestora pode ser configurado para os colaboradores trabalharem remotamente. O plano de ação é de responsabilidade da diretoria de Compliance.

(viii) Contingências de diretores estatutários: caso haja a saída imediata de um diretor estatutário que possui responsabilidades formais perante à CVM, a Citrino pode apontar um diretor substituto até que haja a definição da nova estrutura organizacional. A área de Compliance monitora as certificações e registros CVM e é responsável pelo plano de ação.

Caso haja algum sinistro não identificado nesse plano, a diretoria de Compliance será responsável pelo plano de ação.

Os planos de ação ocorridos serão registrados na ata do comitê de Compliance a critério da diretoria.

Testes periódicos

A Citrino possui rotinas de testes para avaliar os planos de contingências:

(i) Trabalho remoto e rotinas: é realizado trimestralmente um teste de acesso aos principais sistemas (administrador, Bloomberg, Bluedeck, e-mail e VPN) e execução das atividades essenciais, como as atividades do backoffice, em ambiente remoto.

(ii) Data center: é realizado mensalmente um teste de backup com a recuperação de um arquivo aleatório.

(iii) Parque tecnológico: o nobreak principal conta com uma placa de monitoramento para acompanhar o desempenho e é realizado semestralmente uma manutenção preventiva nos equipamentos de energia. A equipe de TI é responsável pela execução dos testes periódicos referentes ao parque tecnológico.

V. POLÍTICA DE SEGURANÇA CIBERNÉTICA

As regras, procedimentos e controles de segurança cibernética da Citrino tem por objetivo assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação da Citrino.

Data center e parque tecnológico

O inventário de ativos (próprios e/ou alugados) relacionados à tecnologia da informação é atualizado pela equipe de TI da Citrino, que provê suporte e planos de manutenção.

Avaliação dos riscos

Em compatibilidade com a estrutura da Citrino entende-se como possíveis cenários de ameaça ataques por qualquer tipo de programas maliciosos como:

(i) Malwares: softwares desenvolvidos para corromper computadores e redes.

(ii) Spyware: software malicioso para coletar e monitorar o uso de informações.

(ii) Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

(iv) Cavalo de troia: aparece dentro de outro software e cria uma porta para a invasão do computador.

Métodos de manipulação para obter informações confidenciais, como senhas e dados pessoais como:

(i) Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento.

(ii) Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais.

(iii) Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais.

Ataques de intrusão da rede (PenTest) burlando o firewall para prejudicar o desempenho ou roubar informações e tentativas de invasão à rede corporativa (cabeada ou WiFi).

Ações de proteção e prevenção

Visando mitigar os riscos identificados, a Citrino tem os seguintes procedimentos, regras e controles:

(i) firewall seguro com rotina quinzenal de atualização;

(ii) antivírus/antimalware/antispyware com proteção real time e varreduras semanais;

(iii) backup dos dados diariamente: interno e cloud;

(iv) 2 (dois) links de internet em load balance;

(v) atualizações diárias dos sistemas operacionais;

(vi) política de conscientização dos usuários com comunicação periódica;

(vii) política de acesso com restrição aos usuários, para que acessem e não alterem a infraestrutura de segurança sem acompanhamento da equipe de TI;

(viii) política de senhas fortes com rotina de alteração periódica;

(ix) identificação por dois fatores;

(x) testes periódicos de invasão na estrutura;

(xi) acompanhamento de logs;

(xii) acesso físico restrito ao CPD;

(xiii) contratação esporádica de consultoria para avaliação da segurança cibernética;

(xiv) controle de acesso à rede wi-fi por mac address control;

(xv) política de desligamento bem definida, visando interromper imediatamente os acessos de usuários desligados; e

(xvi) acesso remoto controlado e autorizado pela administração. Acesso realizado via VPN com criptografia e dois níveis de autenticação.

A diretoria de Compliance é responsável por monitorar a efetividade das ações de proteção e prevenção executadas pela equipe de TI da Citrino.

Plano de ação

Considerando a ocorrência de um sinistro, a equipe de TI da Citrino tem como procedimento:

(i) isolar o problema imediatamente, prevenindo a contaminação de outros sistemas;

(ii) notificar à diretoria de Compliance declarando a classificação do incidente: pequena, moderada, grave e crítica;

(iii) comunicar ao colaborador que sofreu o ataque cibernético, com instruções práticas de como proceder;

(iv) corrigir a falha e aplicar as medidas necessárias para garantir a estabilidade da rede e segurança dos dados.

A diretoria de Compliance deve registrar as informações referentes ao ataque cibernético e o plano de ação efetuado pela equipe de TI na ata do comitê de Compliance subsequente ao evento.

VI. CONSIDERAÇÕES FINAIS

Os resultados relevantes das atividades e eventos de Compliance, bem como recomendações a respeito de eventuais deficiências serão reportados no relatório de controles internos da Gestora. O documento será encaminhado à administração da Citrino até o último dia útil do mês de abril de cada ano relativo ao ano civil anterior.

O conteúdo dessa política consta em um único documento que será atualizado em prazo não superior a 24 (vinte e quatro) meses, ou quando houver alteração na Regulação que demande modificações.

Recomenda-se a leitura desse documento em conjunto com as demais Políticas, Normas, Procedimentos e Manuais da Citrino.

Quaisquer dúvidas em relação ao Manual da Citrino, devem ser encaminhadas à Diretoria de Compliance através do e-mail compliance@citrinogestao.com.br.

* * * * * * *