POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES E SIGILO DAS INFORMAÇÕES

Paraúna Coordenadora de Ofertas Ltda.

CNPJ/MF 61.753.112/0001-08
São Paulo -SP

POLÍTICA DE SEGREGAÇÃO DE ATIVIDADES E SIGILO DAS INFORMAÇÕES

(Art. 20 da Resolução CVM 161)

1. Aplicação

1.1. Esta Política de Segurança e Sigilo das Informações ("Política") deve ser lida, observada e cumprida pela Paraúna Coordenadora de Ofertas Ltda. ("Paraúna") e seus Profissionais (conforme definido abaixo) no exercício da atividade de intermediação de ofertas públicas de distribuição de valores mobiliários, em consonância com o artigo 20 da Resolução da Comissão de Valores Mobiliários ("CVM") nº 161, de 13 de julho de 2022 ("Resolução CVM 161").

1.2. Esta Política se aplica em conjunto e sem prejuízo ao disposto nas demais políticas da Paraúna, incluindo, mas não se limitando, (i) ao Código de Ética para Intermediação de Ofertas Públicas de Distribuição de Valores Mobiliários, (ii) à Política de Subscrição e de Negociação de Valores Mobiliários, (iii) Política de Regras, Procedimentos e Controles Internos e outras políticas e normas internas da Paraúna ("Normativos Paraúna"). Para consultar a versão mais atualizada dos documentos listados acima, os Profissionais da Paraúna devem acessar o site: www.paraunacapital.com.br.

1.3. O disposto nesta Política não prejudica o cumprimento dos demais deveres impostos à Paraúna e aos seus Profissionais pela (i) legislação e regulamentação aplicáveis, tais como os deveres previstos nas normas que coíbem o uso indevido de informação privilegiada, nas normas que disciplinam as ofertas públicas de distribuição de valores mobiliários e na norma que dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, e (ii) autorregulação da ANBIMA – Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais, tais como os deveres previstos em seu "Código de Ética" e seu "Código de Ofertas Públicas".

1.4. Para fins desta Política, entende-se por "Informação Confidencial" as informações confidenciais, reservadas ou privilegiadas independente destas informações estarem contidas em discos, *pen-drives*, fitas, e-mails, outros tipos de mídia eletrônica, em documentos físicos, ou qualquer outro meio de registro, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Paraúna, sobre as suas atividades, seus sócios e clientes, incluindo:

(i) know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

(ii) informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes da Paraúna;

(iii) estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

(iv) informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Paraúna e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, projetos e qualquer outro fato que seja de conhecimento público em decorrência do âmbito de atuação da Paraúna;

(v) informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras da Paraúna, seus sócios e/ou clientes, se aplicável;

(vi) transações realizadas e que ainda não tenham sido divulgadas publicamente;

(vii) quaisquer outras informações obtidas junto a sócios, diretores, funcionários, trainees, estagiários e/ou jovens aprendizes da Paraúna ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral que ainda não tenham sido divulgadas ao público; e

(viii) quaisquer informações que envolvam qualquer decisão de acionista controlador, deliberação da assembleia geral ou dos órgãos de administração, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos seus negócios que possa influir de modo ponderável: (i) na cotação dos valores mobiliários de emissão de certa entidade ou a eles referenciados; (ii) na decisão dos investidores de comprar, vender ou manter aqueles valores mobiliários; ou (iii) na decisão dos investidores de exercer quaisquer direitos inerentes à condição de titular de valores mobiliários emitidos pela entidade ou a eles referenciados.

2. Princípios

2.1. As ações relacionadas com a segurança da informação da Paraúna são norteadas pelos seguintes princípios:

(i) **Confidencialidade:** Garantia de que a informação somente estará disponível e revelada para o usuário previamente autorizado a acessá-la, em função de necessidade de seu exercício profissional contratado pela Paraúna;

(ii) **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que for utilizar um serviço, respeitando os acordos de nível de disponibilidade previamente acertados; e

(iii) **Integridade:** Garantia de que a informação não foi modificada, corrompida por aspectos de ambiente físico ou falhas no ambiente lógico ou destruída de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino.

3. Objetivo

3.1. Esta Política prevê as medidas de segurança da informação e sigilo a serem adotadas e observadas pela Paraúna e seus administradores, empregados e colaboradores ("Profissionais"), que atuam ou venham a atuar na atividade de intermediação de ofertas públicas de distribuição de valores mobiliários, para fins de cumprimento da Resolução CVM 161.

3.2. As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da Paraúna, buscando garantir a proteção de Informações Confidenciais. Todos os Profissionais deverão pautar toda a atividade profissional e as informações da Paraúna e de seus clientes de forma sigilosa, comprometendo-se a transmitir para terceiros, clientes e/ou outros Profissionais apenas as informações estritamente necessárias e relacionadas aos negócios de cada um deles.

4. Conflito de Interesse

4.1. Para fins da presente Política, situações de conflitos de interesses ocorrem quando as atividades desempenhadas pela Paraúna ou pelos seus Profissionais sejam conflitantes com seus próprios interesses pessoais, interesses da Paraúna e/ou interesses dos emissores ou investidores das ofertas públicas.

4.2. Apesar da inexistência de conflito de interesses entre as atividades da Paraúna, na ocorrência de um caso concreto em que seja vislumbrada uma situação de conflito de interesses, os Profissionais devem observar permanentemente a Política de Segregação de Atividades e Sigilo das Informações e reportar o caso imediatamente à Diretoria de Controles Internos e Compliance, que será responsável por determinar medidas mitigatórias ao caso específico, incluindo a restrição de acesso dos envolvidos aos documentos e às informações da oferta em questão. A obrigação de reporte aplica-se a todos os Profissionais da Paraúna.

4.3. Na ocorrência de um caso concreto em que seja identificada situação de conflito de interesses envolvendo a Paraúna e seus Profissionais, caberá à Diretoria de Controles Internos e Compliance avaliar o caso e adotar as medidas legais, regulatórias e disciplinares cabíveis. A referida Diretoria poderá, mediante justificativa fundamentada e a seu exclusivo critério, autorizar a segregação ou o redirecionamento de determinadas atividades, conforme aplicável, observadas as especificidades de cada oferta. Caso necessário, deverá ser promovida a substituição formal dos Profissionais perante a ANBIMA no âmbito da respectiva oferta.

4.4. A Paraúna se compromete a adotar as seguintes medidas para mitigar e identificar possíveis conflitos de interesses, observando a boa-fé e o dever de diligência em suas atividades, incluindo, mas não se limitando, a:

(i) monitoramento de canais de comunicação;

(ii) realização de treinamentos aos Profissionais que utilizem informações e dados sensíveis à Paraúna e a seus clientes; e

(iii) monitoramento contínuo das atividades potencialmente conflitantes para identificar eventual impacto na tomada de decisão dos investidores.

5. Segregação de Atividades

5.1. A Paraúna adota controles internos e procedimentos operacionais, conforme estabelecido em seus Normativos internos, com o objetivo de assegurar a adequada segregação de atividades e mitigar a ocorrência de atos ilícitos, irregularidades ou condutas em desconformidade com a regulamentação aplicável e com as melhores práticas de mercado.

5.2. Nesse contexto, a Paraúna implementa procedimentos específicos relacionados ao tratamento, à proteção e ao compartilhamento de informações confidenciais, bem como mantém barreiras de informação destinadas a controlar e monitorar o fluxo de informações entre suas áreas e atividades, prevenindo o acesso, uso ou divulgação indevidos.

5.3. Assim, quaisquer informações confidenciais relacionadas às atividades desempenhadas pela Paraúna, bem como quaisquer registros mantidos em meio físico ou eletrônico, que tenham sido direta ou indiretamente obtidos, produzidos ou divulgados em razão das atividades exercidas pela Paraúna, deverão ser mantidos sob estrita confidencialidade, sendo vedada sua divulgação a terceiros, inclusive entre Profissionais que exerçam funções distintas no âmbito da própria Paraúna, sem a prévia e expressa autorização da Diretoria de Controles Internos e Compliance.

6. Sigilo e Conduta

6.1. A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros ou Profissionais não autorizados, no caso dos Profissionais não autorizados, não somente durante a vigência de seu relacionamento profissional com a Paraúna, mas também após o seu término.

6.2. Os Profissionais deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento ao disposto nesta Política.

6.3. Sem prejuízo da colaboração da Paraúna com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais e/ou administrativas, deverá ser prévia e tempestivamente informada à Diretoria de Controles Internos e Compliance, para que esta decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

6.4. Caso os Profissionais tenham acesso, por qualquer meio, a uma Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento da Diretoria de Controles Internos e Compliance, indicando, além disso, a fonte da Informação Confidencial assim obtida.

6.5. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou imprudência das pessoas obrigadas a guardar sigilo. Os Profissionais que, desta forma, acessarem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação à Diretoria de Controles Internos e Compliance.

6.6. Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem:

(i) *Insider Trading*, ou seja, a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros;

(ii) "Dica", ou seja, a transmissão, a qualquer terceiro, ou Profissional não autorizado, de Informação Confidencial que possa ser usada na recomendação, na compra e venda de títulos ou valores mobiliários ou na realização de qualquer operação; e/ou

(iii) Front-running, ou seja, a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

6.7. É expressamente proibido valer-se das práticas aqui descritas para obter, para si ou para outrem, vantagem indevida em nome próprio ou de terceiros, oriunda da negociação de títulos e valores mobiliários, sujeitando os Profissionais às penalidades descritas na legislação e regulamentação aplicáveis, incluindo eventual desligamento por justa causa.

6.8. Os Profissionais deverão ler atentamente e entender o disposto nesta Política, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no **Anexo A** ("Termo de Confidencialidade").

7. Controle de Informações

7.1. A Paraúna, possui mecanismos para:

(i) Assegurar o controle de Informações Confidenciais a que tenham acesso seus Profissionais por meio dos sistemas de armazenamento e compartilhamento de documentos que permitam manter histórico de interações com os documentos; e

(ii) Implantar e manter programa de treinamento de Profissionais que tenham acesso a informações relevantes e não públicas.

Barreiras de Informação

7.2. As barreiras de informação são barreiras organizacionais, técnicas e/ou administrativas erguidas entre aqueles que têm acesso regular a informações confidenciais/internas e aqueles que não têm.

7.3. A Paraúna possui barreiras de informação para (incluindo, mas não se limitando a):

- proteger a segurança, a integridade e a confidencialidade das informações;
- gerenciar, proteger e monitorar o fluxo de informações;
- mitigar a troca não autorizada de informações;
- prevenir e gerenciar conflitos de interesse.

7.4. A Paraúna estabelece barreiras de informações entre:

- linhas de negócios que têm acesso apenas a informações públicas; e
- linhas de negócios, departamentos, equipes e Profissionais que, no curso de sua função, atividade ou deveres, têm acesso a informações privilegiadas. Deste lado da barreira da informação podem ser erguidas barreiras adicionais de informações entre departamentos/linhas de negócios.

Wall-Crossing

7.6. Profissionais da Paraúna podem ser autorizados em circunstâncias específicas a divulgar Informações Confidenciais a outros Profissionais para fins comerciais válidos e em conexão com um acordo, transação ou evento específico. Este processo deve estar de acordo com as diretrizes da Paraúna relacionadas ao controle de informações privilegiadas e barreiras da informação, conforme as diretrizes estabelecidas na presente política, e serem autorizadas pela Diretoria de Controles Internos e Compliance.

Acesso aos Sistemas

7.7. Além disso, as instalações da Paraúna são protegidas por controles de acesso apropriados para garantir a segurança dos Profissionais e proteger o sigilo, a integridade e a disponibilidade das Informações Confidenciais.

7.8. A Paraúna conta com estações de trabalho móveis (*notebooks*), com computadores seguros, sendo certo que cada Profissional deverá se certificar de que as sessões abertas e o acesso ao conteúdo armazenado no computador de sua responsabilidade sejam devidamente bloqueados sempre que deixados sem supervisão.

7.9. A Paraúna mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Profissionais. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Paraúna necessária ao exercício de suas atividades. A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Paraúna em caso de violação.

7.10. A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via *webmail*, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

7.11. Para garantir a segurança e integridade das Informações Confidenciais, a Paraúna adota mecanismos robustos para acesso aos sistemas, incluindo autenticação de dois fatores, alteração

periódica de senhas com critérios mínimos de complexidade, bem como monitoramento contínuo de acessos e tentativas de autenticação.

8. Regra Geral de Conduta

8.1. A Paraúna realiza rigoroso controle de acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Profissionais que efetivamente estejam envolvidos em projetos que exijam o seu conhecimento e análise.

8.2. A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos não contiverem informações de clientes ou forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Paraúna. Nestes casos, o Profissional que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a Informação Confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

8.3. A troca de informações entre os Profissionais da Paraúna deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o seu recebimento. Em caso de dúvida a Diretoria de Controles Internos e Compliance deve ser consultada previamente à revelação.

8.4. Neste sentido, os Profissionais não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Paraúna qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente. Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Paraúna.

8.5. Sem prejuízo de a Paraúna manter arquivo físico centralizado, também compete a cada Profissional a responsabilidade pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

8.6. O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham Informações Confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura por pessoas não autorizadas.

8.7. Os Profissionais devem se abster de utilizar *pen drives*, fitas, discos ou quaisquer outros meios de reprodução e/ou armazenamento de informações que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Paraúna. É proibida a conexão de equipamentos na rede da Paraúna que não estejam previamente autorizados pela área de Controles Internos e Compliance.

9. Plano de Identificação de Suspeitas

9.1. Qualquer suspeita de invasão, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Paraúna (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada à Diretoria de Controles Internos e Compliance prontamente, que determinará quais membros da administração da Paraúna e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

9.2. A Diretoria de Controles Internos e Compliance responderá a qualquer informação de suspeita de invasão, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Paraúna, de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de *malware*, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, deverão ser desconectados ou, de outra forma, desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas; e

(vi) Determinação do responsável por arcar com as perdas decorrentes do incidente. A definição ficará a cargo da Diretoria de Controles Internos e Compliance, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

10. Acesso Lógico

10.1. As seguintes diretrizes devem ser consideradas para o acesso lógico à informação:

(i) Os processos de gestão dos acessos lógicos da Paraúna devem ser conduzidos por um time responsável e especializado, que tratará de qualquer sistema, independentemente de ser interno ou em nuvem;

(ii) O acesso a qualquer sistema tecnológico deve ser protegido por credenciais de acesso, certificados, tokens, ou qualquer outro método seguro de identificação e autenticação;

(iii) O acesso às informações e sistemas no âmbito das atividades desempenhadas pela Paraúna devem ser permitidos somente após um processo formal de autorização composto por, no mínimo, um registro feito pelo gestor do Profissional solicitante à área de Controles Internos e Compliance;

(iv) As credenciais de acesso a sistemas e informações, compostas por usuário e senha, devem ser concedidas pela Paraúna a Profissionais e fornecedores somente para o uso em atividades relacionadas a seu trabalho, pelo tempo em que perdurar seu vínculo com a empresa;

(v) Os acessos dos Profissionais e fornecedores devem ser desativados quando eles forem desligados ou tiverem seus contratos de prestação de serviços encerrados;

(vi) Todos os perfis de usuários para acesso às informações ou sistemas de média e alta criticidade devem ser revisados periodicamente pela área de Controles Internos e Compliance, seguindo os critérios de segregação de função e observando o princípio de acesso mínimo e necessidade de conhecimento;

(vii) O acesso lógico aos ativos de tecnologia da informação, tecnologia da automação, sistemas de informação e/ou sistemas técnicos que suportam os processos de negócio da Paraúna deve ser identificado, controlado e protegido;

(viii) Todas as credenciais de acesso devem seguir o princípio de minimização, ou seja, dar acesso ao mínimo necessário para que o Profissional exerça suas funções dentro da Paraúna;

(ix) Identidades de acesso genéricas ou de serviço nos ativos de tecnologia da informação, sistemas de informação e/ou sistemas técnicos que suportam os processos de negócio da Paraúna são permitidas exclusivamente para integrações e/ou conexões; e

(x) Não é permitido que identidades genéricas e de serviços sejam utilizadas por Profissionais ou de fornecedores para fazer acesso a sistemas e/ou demais componentes de tecnologia ou automação. Qualquer exceção deve ser aprovada formalmente pela Diretoria de Controles Internos e Compliance.

11. Análise de Vulnerabilidades Técnicas

11.1. As seguintes diretrizes devem ser consideradas para a análise de vulnerabilidades técnicas:

(i) Deve ser estabelecido um processo de gestão de vulnerabilidades para cobrir todo e qualquer tipo de ativo de tecnologia da informação ("TI") ou tecnologia da automação ("TO");

(ii) Deve ser estabelecida e mantida uma listagem que contemple todos os equipamentos e sistemas críticos da Paraúna, ou seja, aqueles sistemas que mediante falha pode levar a perda econômica significativa, dano físico ou ameaça à vida humana;

(iii) Deve ser garantida a capacidade para prevenção, detecção, resposta e redução de vulnerabilidade a incidentes cibernéticos da Paraúna; e

(iv) Nos casos em que não for possível eliminar totalmente o risco associado às vulnerabilidades de segurança da informação identificadas, devem ser estabelecidos termos de aceitação do risco, nos quais se registrem o motivo, os profissionais aprovadores e a validade do documento.

12. Aquisição, Desenvolvimento e Manutenção Segura de Sistemas de TI e TO

12.1. As seguintes diretrizes devem ser consideradas para aquisição, desenvolvimento e manutenção segura de sistemas de TI e TO:

(i) Os sistemas de informação desenvolvidos ou adquiridos pela Paraúna devem contar com atributos e funcionalidades de segurança que ofereçam proteção adequada às Informações Confidenciais;

(ii) Os requerimentos devem ser identificados e documentados na fase de concepção do sistema, para assegurar que as demandas de segurança aqui previstas sejam atendidas;

(iii) Todo sistema deve ser documentado, tornando sua implantação e operação independentes de conhecimentos informais;

(iv) Os sistemas devem ser protegidos contra alteração indevida, evitando a exposição de dados estratégicos e dados pessoais;

(v) O acesso ao código fonte das aplicações deve ser adequadamente protegido;

(vi) Dados pessoais ou dados pessoais sensíveis reais não devem ser utilizados em ambientes de teste, homologação e aplicativos. Neste caso, os dados utilizados em ambientes não produtivos devem estar anonimizados;

(vii) Fornecedores e Profissionais que desenvolvam sistemas para uso da Paraúna devem assinar termos de responsabilidade, e se submeterem a todas as políticas de segurança pertinentes;

(viii) O desenvolvimento de sistemas deve seguir as boas práticas de mercado referentes ao desenvolvimento seguro;

(ix) Os ambientes de desenvolvimento, teste e produção devem ser segregados física ou logicamente, evitando o acúmulo de acessos de desenvolvedores ao ambiente de produção;

(x) Devem ser estabelecidos requisitos de segurança necessários para a aquisição ou desenvolvimento de novos sistemas para qualquer ambiente, assim como as possíveis alterações e/ou atualizações em sistemas devem atender aos requisitos de segurança estabelecidos;

(xi) As aquisições de software e sistemas de TI e TO, assim como o desenvolvimento e manutenção de ativos tecnológicos, devem garantir a adoção e a manutenção dos requisitos previamente definidos nas *baselines*, padrões e normas de segurança cibernética definidas pela Paraúna;

(xii) Deve-se estabelecer um processo de validação dos requisitos de segurança na análise crítica de novas soluções para TI e TO, assim como na análise crítica de soluções existentes que sofreram alterações significativas; e

(xiii) Os requisitos de segurança necessários para assegurar a confidencialidade, integridade, disponibilidade e conformidade de sistemas e dados do ambiente operacional devem ser garantidos.

13. Backup, Arquivamento e Restauração

13.1. As seguintes diretrizes devem ser consideradas para fins de backup, arquivamento e restauração:

(i) Um plano de backup deve ser criado para atender os requisitos de retenção e guarda de dados da Paraúna, conforme os requisitos de negócio;

(ii) Os resultados dos backups devem ser periodicamente validados, com frequência adequada e possíveis falhas identificadas devem ser reportadas como incidentes;

(iii) O processo de restauração deve ser testado nos sistemas críticos de forma amostral, no mínimo, anualmente. Casos em que não seja tecnicamente possível a sua execução, devem ter controles compensatórios; e

(iv) O tempo de vida do backup deve levar em consideração as necessidades do negócio e as exigências legais e regulatórias.

14. Classificação da Informações Relacionadas aos Ambientes de TI e TO

14.1. As seguintes diretrizes devem ser consideradas para a classificação das informações relacionadas aos ambientes de TI e TO:

(i) Todas as informações da Paraúna devem ser atribuídas a um proprietário formalmente designado;

(ii) Todas as informações devem ser classificadas de acordo com seu valor, grau de sigilo, criticidade e sensibilidade perante o negócio, de forma que sejam adotados os mecanismos de proteção adequados, balanceando custo e complexidade do controle, sendo que as Informações Confidenciais terão tratamento em conformidade com esta Política;

(iii) Devem ser atribuídas às informações sem classificação explícita um grau de confidencialidade elevado, não sendo permitido o seu repasse ou divulgação para qualquer pessoa que não seja da Paraúna, exceto quando se tratar de informações públicas e de mercado devidamente autorizadas nos termos desta Política; e

(iv) Todos os Profissionais devem tratar as informações da Paraúna de acordo com seu nível de classificação, de forma a protegê-las contra atos ou acessos indevidos, ou divulgação não autorizada.

15. Continuidade de Negócio, Recuperação de Desastre e Crise Cibernética

15.1. As seguintes diretrizes devem ser consideradas para continuidade de negócio, recuperação de desastre e crise cibernética:

(i) Devem ser mantidos planos específicos de gerenciamento de crise e planos de recuperação que atendam aos ambientes de TI e TO da Paraúna, esses deverão ser testados para garantir a continuidade operacional das atividades críticas, através da recuperação e restauração das operações, em caso de catástrofe, desastres ou interrupção dos serviços e processos críticos de TI e TO;

(ii) Deve-se garantir que todas as recomendações identificadas nos resultados dos testes/simulações sejam avaliadas, priorizadas e implantadas. E quando se tratar melhorias de processos, que os mesmos sejam padronizados;

(iii) Deve-se formalizar com as áreas de negócio a priorização de recuperação dos ambientes de TI e TO, tomando como base o plano de continuidade de negócios feitos pelas áreas de negócio da Paraúna; e

(iv) Recomenda-se a criação de *playbooks* para os cenários críticos de indisponibilidade dos ambientes de TI e TO.

16. Vigência e Atualização desta Política

Esta Política foi elaborada e aprovada pela Diretoria da Paraúna e somente poderá ser modificada por deliberação da Diretoria da Paraúna.

Esta Política entra em vigor a partir da data de habilitação da Paraúna para atuar como coordenadora de ofertas públicas.

17. Dúvidas e Comentários

Em caso de dúvidas ou comentários a respeito do conteúdo desta Política, os Profissionais da Paraúna devem entrar em contato com a Diretoria de Controles Internos e Compliance no endereço eletrônico compliance@paraunacapital.com.br.

ANEXO A

Termo de Confidencialidade

Eu, _____, CPF/MF nº _____, declaro, para os devidos fins, que (i) recebi um exemplar da Política de Segurança e Sigilo das Informações da Paraúna Coordenadora de Ofertas Ltda. ("Política"), (ii) estou ciente do seu teor e de pleno acordo com seu conteúdo, comprometendo-me a cumpri-la, fielmente, durante toda a vigência das minhas atividades relacionadas à intermediação de ofertas públicas de distribuição de valores mobiliários e, após esse período, no que for cabível e (iii) tenho conhecimento que as infrações à Política estão sujeitas a ações disciplinares, independentemente do nível hierárquico, sem prejuízo das penalidades cabíveis.

São Paulo, [•] de [•] de [•].

_____

Assinatura