



Política de Regras, Procedimentos e Controles Internos

Junho de 2026

ÍNDICE

1. INTRODUÇÃO E OBJETIVOS.....	4
2. ABRANGÊNCIA.....	4
3. ACOMPANHAMENTO DAS REGRAS ESTABELECIDAS NOS MANUAIS E POLÍTICAS.....	4
3.1. Diretor de Compliance.....	5
4. NORMAS DE CONDUTA.....	6
5. POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO	7
5.1. Informações Confidenciais e Privilegiadas.....	7
5.1.1. Informação Privilegiada	9
5.1.2. Insider Trading e “Dicas”	9
5.1.3. Front-Running.....	9
5.2. Princípios Gerais de Uso e Segurança da Informação	10
5.3. Propriedade Intelectual	12
5.4. Segurança dos Ambientes Físicos	12
5.5. Segurança do Ambiente Lógico.....	13
5.5.1. Sistemas/Softwares	13
A Gerência de Tecnologia poderá valer-se deste instrumento para desinstalar, sem prévio aviso, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).....	14
5.5.2. Estações de Trabalho	14
5.5.3. Equipamentos Particulares ou de Terceiros na Strata	15
5.5.4. Dispositivos de Armazenamento Móvel	15
5.5.5. Ferramentas de Comunicação.....	16
5.6. Gerenciamento de Senhas e Autenticação.....	16
5.7. Correio Eletrônico (E-mail).....	17
5.8. Acesso à Rede Corporativa.....	19
5.9. Acesso à Internet.....	20
5.10. Retenção de Dados	21
5.11. Gestão de Incidentes.....	22
5.12. Proteção de Dados e Auditoria	26
5.13. Papéis e Responsabilidades.....	26
5.13.1. Todos os Usuários (funcionários, estagiários, prestadores de serviços):.....	26
5.13.2. Gestores:	27
5.13.3. Gerência de Tecnologia:	28
5.13.4. Programa de Treinamento e Capacitação em Segurança da Informação: A Strata manterá um programa permanente de treinamento e capacitação em segurança e sigilo das informações, em conformidade com o disposto no art. 24 da Resolução CVM 21.....	28
O programa de treinamento deverá observar as seguintes disposições:	29
5.13.5. Gerência de Recursos Humanos:.....	29
5.14. Violação da Política de Confidencialidade e Segurança da Informação	29
5.15. Boas Práticas	30
5.16. Canais de Comunicação	30
6. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES.....	30
7. TRATAMENTO DE CONFLITO DE INTERESSES.....	31
7.1. Operações entre Veículos de Investimentos e Empresas Relacionadas.....	32

7.2.	Disclosure aos clientes.....	32
8.	POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO.....	32
8.1.	Princípios Gerais.....	32
8.2.	ABR.....	33
8.2.1.	Colaboradores	33
8.2.2.	Serviços Prestados.....	34
8.2.3.	Produtos Oferecidos	34
8.2.4.	Cotistas	35
8.2.5.	Prestadores de Serviços Relevantes.....	35
8.2.6.	Ativos.....	37
8.3.	Comunicação COAF.....	38
8.4.	Indicadores de Eficácia.....	41
8.4.1.	Pessoas Politicamente Expostas	41
8.5.	Treinamentos.....	Erro! Indicador não definido.
8.6.	Avaliação Interna e Periódica de Risco.....	43
9.	POLÍTICA ANTICORRUPÇÃO.....	43
9.1.	Introdução.....	44
9.2.	Abrangência das Normas de Anticorrupção	44
9.3.	Definição	44
9.4.	Normas de Conduta	45
10.	VANTAGENS, BENEFÍCIOS E PRESENTES	46
10.1.	Vantagens e Benefícios Proibidos	46
11.	PROGRAMA DE TREINAMENTO	48
12.	PENALIDADES PARA DESVIOS DE CONDUTA DOS COLABORADORES	49
	Anexo I.....	50
	Anexo II	53
	Anexo III.....	54
	Anexo IV	55
	Anexo V.....	56
	Anexo VI	57
	Anexo VII	59

1. INTRODUÇÃO E OBJETIVOS

Esta Política de Regras, Procedimentos e Controles Internos ("Política") tem por objetivo estabelecer regras e procedimentos, bem como descrever os controles internos a serem implementados e observados pelas empresas do Grupo Strata ("Strata") e pelos seus Colaboradores (conforme definidos abaixo).

A Strata presta serviços de administração de carteiras de valores mobiliários, que consiste no exercício profissional de atividades relacionadas, direta ou indiretamente, ao funcionamento, à manutenção e à gestão de carteiras de valores mobiliários, incluindo a aplicação de recursos no mercado de valores mobiliários por conta do investidor, nos termos da Resolução da Comissão de Valores Mobiliários ("CVM") n.º 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21").

Além disso, a Strata também presta serviços relacionados à aquisição e vinculação a um patrimônio separado de direitos creditórios, com o objetivo de lastrear a emissão de valores mobiliários, tais como aqueles previstos nas regulamentações específicas de securitização, desde que não configurem atividade regulamentada privativa de companhia securitizadora junto à CVM.

As regras e procedimentos aqui previstos visam garantir o atendimento às normas, políticas e regulamentações vigentes, referentes à atividade de gestão de carteiras de valores mobiliários, à atividade de securitização e aos padrões ético e profissional exigidos pela Strata no bom exercício de suas atividades. Dessa forma, objetivam facilitar a identificação de eventos, reduzir a frequência de surgimento de eventos, e mitigar riscos decorrentes de eventos quando estes surgirem, bem como, disseminar a cultura de controles para garantir o cumprimento das normas contidas na Resolução CVM 21, como nas demais normas aplicáveis estabelecidas pelos órgãos reguladores e autorreguladores.

A presente Política deve ser lida em conjunto com o Código de Ética e Conduta da Strata ("Código de Ética") e as demais políticas da Strata ("Manuais e Políticas da Strata"), observado que todos os termos iniciados em letra maiúscula que não forem aqui definidos têm seu significado atribuído no Código de Ética e Conduta da Strata.

2. ABRANGÊNCIA

Esta Política aplica-se à Strata e a todos os seus colaboradores. Para os fins desta Política, são considerados colaboradores da Strata todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, profissional, contratual, ou de estágio com a Strata ("Colaboradores").

3. ACOMPANHAMENTO DAS REGRAS ESTABELECIDAS NOS MANUAIS E POLÍTICAS

A coordenação direta das atividades relacionadas a esta Política é uma atribuição do Diretor de Riscos e Compliance da Strata, conforme indicado em seus documentos societários ("Diretor de Compliance"), bem como a sua implementação e divulgação, garantindo que todos os Colaboradores conheçam seu conteúdo.

A violação dos preceitos desta Política poderá resultar na aplicação de advertência, suspensão ou demissão determinada pelo Diretor de Compliance, de acordo com a gravidade de cada ato praticado, conforme previsto no item 12 desta Política.

O Diretor de Compliance exerce suas funções com plena independência, não estando sujeito a qualquer ingerência por parte da equipe de gestão, e é o responsável pela implementação dos procedimentos previstos nesta Política.

3.1. Diretor de Compliance

São atribuições do Diretor de Compliance, sem prejuízo das demais descritas nesta Política:

- a) Definir os princípios éticos a serem observados por todos os Colaboradores constantes dos Manuais e Políticas da Strata, discutindo e elaborando sua revisão periódica;
- b) Conduzir avaliações de processos, no mínimo, anualmente, para verificação e acompanhamento dos procedimentos de controles internos estabelecidos nesta Política, e envio aos órgãos de administração da Strata, até o último dia útil do mês de abril de cada ano, de um relatório relativo ao ano civil imediatamente anterior à data da entrega, contendo **(1)** as conclusões dos exames efetuados; **(2)** as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronograma de saneamento delas, quando for o caso; e **(3)** a manifestação do diretor responsável pela atividade de securitização a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las;
- c) Promover a disseminação de padrões éticos e de integridade, de modo a demonstrar a todos os Colaboradores a importância dos controles internos e o papel de cada um no processo;
- d) Conduzir inspeções com base em sistemas de monitoramento eletrônico e telefônico, conforme as determinações da Política de Confidencialidade e Segurança da Informação, disposta no item 5 abaixo, independentemente da ocorrência ou suspeita de descumprimento de quaisquer das regras estabelecidas nos Manuais e Políticas da Strata, a fim de evitar descumprimento das regras da Strata, sem que isto represente invasão de privacidade;
- e) Assegurar que os Colaboradores não negociem, em nome próprio ou de terceiros, valores mobiliários e ativos financeiros que não estejam em conformidade com as determinações da Política de Compra e Venda de Valores Mobiliários da Strata;
- f) Analisar situações que possam ser caracterizadas como conflitos de interesse pessoais e profissionais, conforme delineado no Código de Ética, na Política de Compra e Venda de Valores Mobiliários da Strata e nesta Política, e solicitar a tomada das devidas providências nos casos de caracterização de conflitos de interesse ou de

qualquer outro descumprimento às normas definidas nos Manuais e Políticas da Strata;

- g) Apreciar todos os casos que cheguem ao seu conhecimento sobre quaisquer suspeitas ou indício de condutas contrárias aos Manuais e Políticas da Strata, e apreciar e analisar situações não previstas, bem como definir as sanções a ser aplicadas;
- h) Assegurar o cumprimento das determinações legais e regulatórias em vigor sobre a Prevenção à Lavagem de Dinheiro e do Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, disposta no item 8 abaixo, e a prevenção da utilização dos ativos e sistemas da Strata para fins ilícitos;
- i) Ministrando treinamentos a todos os Colaboradores, promovendo a ampla divulgação dos Manuais e Políticas da Strata a todos os Colaboradores e abrangendo todos os temas abordados nesta Política;
- j) Tratar todos os assuntos que cheguem ao seu conhecimento com sigilo, preservando a imagem dos Colaboradores e da Strata, salvo nas hipóteses previstas na regulação e na autorregulação, sendo vedado qualquer tipo de retaliação; e
- k) Mediante ocorrência ou suspeita de descumprimento de quaisquer regras estabelecidas nos Manuais e Políticas da Strata, utilizar registros e sistemas de monitoramento para verificar a conduta dos Colaboradores envolvidos e enviar as denúncias de forma sigilosa ao órgãos internos da Strata aplicáveis; e
- l) Solicitar sempre que necessário, para a análise de suas questões, o apoio da auditoria interna ou externa ou outros assessores profissionais, incluindo, a análise de recebimento de vantagens, benefícios e presentes, conforme previsto item 10 abaixo.

Além da supervisão do Diretor de Compliance, a fiscalização dos Colaboradores também é responsabilidade de cada Colaborador, que está obrigado a relatar imediatamente ao Diretor de Compliance qualquer irregularidade na conduta de outros Colaboradores ou terceiros que tenha ciência.

É vedado ao Diretor de Compliance:

- a) Acumular posição com a do diretor responsável pelas atividades de gestão ou de securitização; e
- b) Atuar em qualquer atividade que limite sua independência, na Strata, ou fora dela.

4. NORMAS DE CONDUTA

Todos os Colaboradores deverão seguir normas de conduta, delineadas no Código de Ética da Strata, e os princípios éticos no desempenho de suas atividades, perante colegas de trabalho, clientes, prestadores de serviços e demais contrapartes, na condução dos negócios da Strata. O Código de Ética também contém os valores da Strata: equipe, integridade, compromisso e confidencialidade.

Os Colaboradores devem respeitar todas as normas e legislação vigente que regulam o exercício das atividades da Strata, em especial Leis Anticorrupção, conforme disposto no item 9 abaixo. É extremamente prejudicial à reputação e aos resultados da Strata ter seu nome ligado a qualquer tipo de processo administrativo, sanção ou condenação por atitudes tomadas por qualquer Colaborador em desacordo com as leis, especialmente aqueles em posição de gerência ou diretoria, a quem cabe dar o exemplo aos demais e reforçar que as operações devem ser feitas de forma transparente e sem conflitos.

Neste sentido, todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis, bem como do completo conteúdo desta Política. Em caso de dúvidas ou necessidade de aconselhamento, é imprescindível que se busque auxílio imediato junto ao Diretor de Compliance.

Os Colaboradores devem manter um bom relacionamento com os clientes, concorrentes, fornecedores, investidores e demais contrapartes, e um bom ambiente de trabalho, privilegiando o trabalho em equipe, cordialidade, respeito aos colegas e abertura para a diversidade de opiniões, com tratamento justo e equitativo, sendo vedado qualquer tipo de discriminação ou difamação em função de raça, cor, sexo, credo ou qualquer outro fator.

Os Colaboradores também devem agir com diligência e cuidado na condução de suas atividades, devendo evitar ações que possam colocar em risco o patrimônio e imagem da Strata e de seus clientes. O Colaborador deve usar também a estrutura tecnológica da Strata (e-mail, internet, telefone, dentre outras) exclusivamente para fins profissionais.

5. POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

5.1. Informações Confidenciais e Privilegiadas

Todos os Colaboradores deverão seguir as regras de confidencialidade com o intuito de preservar informações confidenciais, cujo conceito deve ser entendido como quaisquer informações que a Strata ou seus clientes forneçam aos Colaboradores que não sejam de domínio público, não tenham sido divulgadas ao mercado, ou que a Strata não deseje que sejam divulgadas. São exemplos de informações confidenciais, independente destas informações estarem contidas em discos, disquetes, pen- drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Strata, seus sócios e clientes, que não devem ser divulgadas a terceiros, como:

- a) Informações sobre os negócios da Strata, seus clientes, investimentos, estruturas societárias, custos, preços, lucros, relatórios financeiros, produtos, serviços, equipamentos, sistemas, procedimentos, operações, planos de negócios, operações financeiras e contratos;
- b) Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- c) Informações técnicas, financeiras ou relacionadas a estratégias de investimento e desinvestimento ou comerciais; incluindo saldos, extratos e posições de clientes dos

fundos de investimento e carteiras administradas geridos pela Strata;

- d) Informações sobre operações estruturadas, demais operações e seus respectivos valores analisadas ou realizadas pelos fundos de investimento e carteiras administradas geridos pela Strata;
- e) Informações técnicas, financeiras ou relacionadas a credores e devedores de direitos creditórios adquiridos para utilização como lastro de emissão de títulos de securitização;
- f) Relatórios, estudos, opiniões internas sobre ativos financeiros;
- g) Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
- h) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Strata e a seus sócios ou clientes;
- i) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos de investimento geridos pela Strata;
- j) Informações sobre transações realizadas e que ainda não tenham sido divulgadas publicamente; e
- k) Outras informações obtidas junto a Colaboradores ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

Não é permitido o uso indevido ou a divulgação de informações confidenciais obtidas por qualquer meio, seja ele contratual, advindo do relacionamento com cliente, referente a investimentos das carteiras ou fundos de investimento geridos pela Strata ou referente a operações de securitização realizadas pela Strata. Informações consideradas confidenciais devem ser acessadas apenas por Colaboradores devidamente autorizados que necessitem de tal acesso para a execução de suas atividades, de forma a preservar ao máximo o seu caráter restrito. Informações confidenciais deverão ser utilizadas exclusivamente para o cumprimento das atividades na Strata e os Colaboradores obrigam-se a não compartilhar tal informação com terceiros.

Eventuais terceiros que tenham acesso a qualquer informação confidencial estão também sujeitos aos mesmos deveres e obrigações de sigilo.

É vedado aos Colaboradores, mesmo após o fim do vínculo de trabalho deste com a Strata, o uso ou divulgação de qualquer informação ou dado ao qual teve acesso em função de suas atividades na Strata, exceto caso, à época, tais dados já sejam de domínio público.

Caso seja determinada a revelação de alguma das informações delineadas nesta Política por alguma autoridade governamental ou em virtude de decisões judiciais, arbitrais ou administrativas, a decisão deverá ser comunicada previamente ao Diretor de Compliance, que decidirá sobre a maneira mais adequada de proceder com a revelação.

5.1.1. Informação Privilegiada

Para fins desta Política de Confidencialidade e Segurança da Informação, considera-se informação privilegiada qualquer informação relevante a respeito de qualquer companhia, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros).

Exemplos de informações privilegiadas são informações verbais ou documentadas a respeito de resultados operacionais de empresas, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), e qualquer outro fato que seja objeto de um acordo de confidencialidade firmado por uma empresa com a Strata ou com terceiros.

As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

5.1.2. Insider Trading e “Dicas”

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores).

“Dica” é a transmissão, a qualquer terceiro, estranho às atividades da Strata, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários. A prática de *Insider Trading* e de “Dica” são totalmente vetadas pela Strata.

5.1.3. Front-Running

Front-running significa a prática que envolve aproveitar alguma informação privilegiada para realizar ou concluir uma operação antes de outros.

O disposto nos itens de “*Informação Privilegiada*”, “*Insider Trading e Dicas*” e “*Front-running*” deve ser analisado não só durante a vigência de seu relacionamento profissional com a Strata, mas também após o seu término.

Os Colaboradores deverão guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, 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.

Caso os Colaboradores tenham acesso, por qualquer meio, a informação privilegiada não autorizada, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance, indicando, além disso, a fonte da informação privilegiada assim obtida. Tal dever de comunicação também será aplicável nos casos em que a informação privilegiada seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessem a informação privilegiada, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de

Compliance anteriormente mencionada.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas no item 12 abaixo e na legislação aplicável, incluindo eventual demissão por justa causa.

5.2. Princípios Gerais de Uso e Segurança da Informação

Todas as informações, os dados e os sistemas de informação produzidos e/ou utilizados internamente pelos Colaboradores devem ser considerados como ativos que tem valor para a Strata e se constituem em vantagem competitiva, devendo ser protegidos contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças, de modo a reduzir riscos e garantir a continuidade dos negócios da Strata. A proteção dessas informações, dados e sistemas de informação, através da adoção dos procedimentos delineados nesta Política de Confidencialidade e Segurança da Informação, é responsabilidade e obrigação de todos os Colaboradores, e uma prioridade para a Strata.

Os Princípios Gerais de Segurança da Informação valorizados pela Strata são:

- a) **Autenticidade:** garante a identidade de quem está enviando a informação, ou seja, propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mudanças ao longo de um processo;
- b) **Confidencialidade:** a garantia de que a informação é acessível somente às pessoas com acesso autorizado;
- c) **Integridade:** a salvaguarda da exatidão e integralidade da informação e dos métodos de processamento; e
- d) **Disponibilidade:** garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação (Strata).

Todos os Ativos de TIC de propriedade e/ou sob responsabilidade da Strata devem ser usados para fins profissionais, exceto para os casos explicitados nesta Política de Confidencialidade e Segurança da Informação, e utilizados de forma lícita, ética e moral, seguindo as regras da Strata. O uso indiscriminado dos dispositivos corporativos para fins pessoais deve ser evitado e nunca dever ser prioridade em relação a qualquer utilização profissional.

Os sistemas corporativos e o e-mail corporativo são gravados e ficam registrados nos servidores, disponíveis para eventuais inspeções do Diretor de Compliance.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam prejudicar a imagem e afetar a reputação da Strata.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da Strata, bem como avisar prontamente o Diretor de Compliance.

A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

A Strata realizará o controle de acessos aos Ambientes Físicos e aos Ambientes Lógicos da Strata, devendo os Usuários respeitar as regras impostas e vinculadas a cada acesso fornecido. As autorizações devem ser revistas, confirmadas e registradas continuamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

É fundamental para a proteção e salvaguarda das informações que os Usuários adotem a ação de **COMPORTAMENTO SEGURO** e **CONSISTENTE** com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

A interpretação da presente Política de Confidencialidade e Segurança da Informação, bem como dos documentos correlatos, deverá ser feita de forma restritiva.

Sendo assim, caso alguma atividade não esteja abarcada pelos documentos mencionados, esta deverá ser submetida a um processo de validação formal por parte do gestor, do Colaborador ou do terceiro, antes de sua execução.

A contratação de Colaboradores e terceiros que envolvam o compartilhamento de informações de propriedade e/ou sob responsabilidade da Strata deverá ser acompanhada de termos de confidencialidade e cláusulas contratuais relativas à segurança da informação.

A Strata adota um mecanismo e processo de salvaguarda (*backup*) completa de seus sistemas com fins de conformidade com requisitos legais, operacionais e de lógica de negócio. No caso de falhas ou incidentes de segurança da informação, será realizada a recuperação das informações através desses backups.

A Strata possui um canal de comunicação de incidentes, cuja divulgação é realizada junto a seus colaboradores para o reporte de incidentes de segurança da informação, através do e-mail tecnologia@stratacapital.com.br

A Strata respeita os regulamentos e leis relativos à proteção da privacidade e dados pessoais do Brasil, assim como demais normas relacionadas, adotando uma postura de conformidade com as boas práticas e medidas de segurança em privacidade e proteção de dados pessoais.

Todas as dúvidas relacionadas a esta Política de Confidencialidade e Segurança da Informação deverão ser encaminhadas à Área de Tecnologia da Informação, através do e-mail tecnologia@stratacapital.com.br.

5.3. Propriedade Intelectual

Todos os documentos, arquivos e informações acessadas, manuseadas, armazenadas ou descartadas durante a atividade dos Usuários, bem como os demais ativos intangíveis e tangíveis disponibilizados, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Strata, tais como minutas de contrato, cartas, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise de gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Strata, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Strata, devendo todos os documentos permanecer em poder e sob a custódia da Strata, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Strata, salvo se autorizado expressamente pela Strata e ressalvado o disposto abaixo.

Toda e qualquer utilização de obras intelectuais, softwares, desenhos industriais, marcas, identidades visuais e/ou quaisquer outros sinais distintivos atuais ou futuros da Strata são de propriedade intelectual da Strata.

Caso um Colaborador, ao ser admitido, disponibilize à Strata documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à Strata, este anui que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Strata, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Strata, exceto se aprovado expressamente pela Strata.

5.4. Segurança dos Ambientes Físicos

Todos os equipamentos de TI da Strata (servidores, notebooks, etc) são inventariados e identificados como patrimônio da empresa de forma única e individual, salvo itens de baixo valor, tais como mouse, teclado, nobreak, e etc., e sua utilização é restrita aos usuários autorizados.

A entrada nas áreas de armazenamento de ativos (Data Center) tem acesso devidamente controlado e monitorado. A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviços, e até mesmo funcionários sem acesso liberado) será sempre acompanhada de pessoas autorizadas.

Os ativos que ofereçam risco à Segurança da Informação podem ser temporariamente

desativados pela Gerência de Tecnologia.

Os ativos de TI são disponibilizados aos usuários, de acordo com os cargos ocupados, para que possam desempenhar suas funções, mediante assinatura do “TERMO DE RECEBIMENTO E COMPROMISSO DA POLÍTICA DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS DA STRATA”, como consta no Anexo II, e “CONTRATO DE COMODATO”, como consta no Anexo III.

Para disponibilização de ativos à terceiros há necessidade de aprovação da área da Strata atendida, mediante análise da real necessidade para o desempenho da atividade.

Os dispositivos móveis, tais como notebooks e celulares, serão disponibilizados aos usuários que necessitem de mobilidade ou que sejam elegíveis à Política de Trabalho Híbrido – Home Office e Presencial.

A utilização de qualquer ativo, de propriedade da Strata, poderá ser suspensa ou monitorada quando houver qualquer indício de utilização ou compartilhamento inapropriado, ou ainda vazamento de informações que estiverem sob a responsabilidade do usuário.

Os ativos de propriedade da Strata devem ser devolvidos pelo usuário em caso de desligamento ou sempre que solicitado pela Gerência de Tecnologia.

Os ativos sob a responsabilidade dos usuários não podem ser compartilhados com terceiros (incluindo familiares).

Quando aplicável, os ativos descontinuados devem ter seus dados apagados, sobrescritos ou até mesmo os respectivos discos de memória (HD) serem removidos pela equipe do Help Desk.

O uso dentro das instalações da Strata, de quaisquer equipamentos de gravação, fotografia, som ou outro tipo de equipamento similar, somente poderá ser realizado a partir da autorização do gestor responsável pela área de atividade.

5.5. Segurança do Ambiente Lógico

5.5.1. Sistemas/Softwares

As estações de trabalho, incluindo notebooks, devem conter exclusivamente softwares licenciados e homologados. O padrão de configuração dessas estações é definido pela Gerência de Tecnologia e não pode ser modificado sem autorização da mesma.

A atualização de Dispositivos de Armazenamento Móvel é permitida dentro dos limites estabelecidos por esta Política de Confidencialidade e Segurança da Informação e poderá ser monitorada pela Gerência de Tecnologia. Vale salientar que o Usuário é responsável pelos danos causados por possíveis vírus ou outras ameaças que tais dispositivos possam conter.

Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários autorizados ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

Não é permitida a execução de programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total dos arquivos ou a indisponibilidade de serviços.

Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da Strata.

Não enviar informações confidenciais para e-mails externos (não corporativos) ou através de e-mails externos (particulares).

As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis. A documentação dos sistemas deve ser mantida atualizada. A cópia de segurança deve ser testada regularmente, por amostragem, e mantida atualizada.

O acesso aos sistemas é permitido somente após a autenticação do Usuário.

As credenciais de acesso são de uso pessoal, nominativas, intransferíveis e de responsabilidade exclusiva dos usuários.

É proibida qualquer tentativa de acesso não autorizado aos sistemas da Strata.

As licenças para utilização dos sistemas são concedidas pela empresa aos usuários que necessitem dos recursos para desempenho das suas funções. A utilização poderá ser monitorada, e a licença suspensa, a qualquer momento, por decisão da Gerência de Tecnologia.

Qualquer software que, por necessidade do trabalho tiver que ser instalado, deverá ser avaliado pela Gerência de Tecnologia, para que o mesmo possa ser homologado e só assim serem disponibilizados aos usuários da área solicitante.

A empresa reconhece os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, coibindo e monitorando o eventual uso indevido de programas não licenciados. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na Strata.

A Gerência de Tecnologia poderá valer-se deste instrumento para desinstalar, sem prévio aviso, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

5.5.2. Estações de Trabalho

As Estações de Trabalho possuem códigos internos, os quais permitem que elas sejam identificadas. Desta forma, tudo o que for executado na Estação de Trabalho é de responsabilidade do Usuário.

No caso de uma Estação de Trabalho ser realocada para outro usuário, esta será formatada e todos os dados serão apagados.

A atualização de Dispositivos de Armazenamento Móvel é permitida dentro dos limites estabelecidos por esta Política de Confidencialidade e Segurança da Informação e poderá ser

monitorada pela Gerência de Tecnologia. Vale salientar que o usuário é responsável pelos danos causados por possíveis vírus ou outras ameaças que tais dispositivos possam conter.

A Gerência de Tecnologia não realiza cópias de segurança das informações armazenadas localmente nas estações de trabalho. As cópias de segurança (backup's) são realizadas somente nas informações armazenadas nos Servidores Corporativos (diretórios de rede Público, Corporate, etc.). Desta forma, é de responsabilidade do usuário manter os arquivos de trabalho armazenados corretamente nos Servidores Corporativos.

O acesso a Estação de Trabalho deverá ser encerrado no final do expediente, quando o Usuário deverá desconectar o seu acesso à VPN e desligar o equipamento.

Antes de se afastar da Estação de Trabalho, o Usuário deverá obrigatoriamente, bloquear a Estação de Trabalho.

Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízos à Strata, só devem ser utilizadas em equipamentos com controles adequados.

Apenas o pessoal autorizado pela Gerência de Tecnologia pode instalar softwares nas estações de trabalho dos usuários e devem utilizar apenas softwares licenciados pela Strata. Em caso de dúvidas, favor consultar a área de TI através dos canais de suporte (Help Desk).

A Gerência de Tecnologia deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

5.5.3. Equipamentos Particulares ou de Terceiros na Strata

Notebooks particulares ou de terceiros para serem utilizados na rede corporativa precisam, obrigatoriamente, ser avaliados e aprovados pela Gerência de Tecnologia.

É de responsabilidade da área contratante de prestadores de serviços, incluir no contrato entre as partes uma cláusula declarando a responsabilidade da empresa terceira sobre todo e qualquer software instalado nos equipamentos dos mesmos. Sugere-se a reavaliação semestral dos equipamentos.

É de responsabilidade da área contratante encaminhar os equipamentos de terceiros sob sua responsabilidade para o Help Desk para que sejam verificadas as atualizações de antivírus, existências de vírus e a instalação de certificado para acesso à rede corporativa.

5.5.4. Dispositivos de Armazenamento Móvel

O uso de Dispositivos de Armazenamento Móveis não é estimulado na empresa, devendo ser tratado como exceção.

Informações devem ser transmitidas usando as ferramentas corporativas disponíveis (e-mail, diretório temporário, OneDrive) que mantém a segurança requerida.

Caso seja necessário transportar arquivos através de Dispositivos de Armazenamento

Móveis (HD Externo ou PenDrive), o processo deve ser liberado pela Gerência de Tecnologia. Recomenda-se que as informações sejam criptografadas e apagadas logo após o transporte, a fim de evitar vazamentos de informações.

No caso de comprovação de utilização de Dispositivos de Armazenamento Móveis sem autorização, o Usuário será responsabilizado no caso de perda/vazamento de informação ou no caso de entrada de vírus ou softwares maliciosos na rede corporativa da Strata.

5.5.5. Ferramentas de Comunicação

Recomenda-se a utilização do Microsoft Teams como ferramenta de comunicação, devendo ser utilizado prioritariamente para atividades de negócios, podendo ser monitorado e utilizado para fins de auditoria.

Toda e qualquer gravação realizada através da ferramenta de comunicação deve ser avisada e aprovada pelos participantes da reunião, tendo em vista o regramento previsto na LGPD (Lei Geral de Proteção de Dados).

5.6. Gerenciamento de Senhas e Autenticação

Todo Usuário deverá ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo de sua senha pessoal, não podendo em hipótese alguma repassar a mesma para outros Usuários ou terceiros.

A senha do Usuário deverá conter no mínimo 08 (oito) caracteres, devendo conter letras, números e caracteres especiais e não se deve repetir as 5 (cinco) últimas senhas.

A senha deve ser alterada, no mínimo, a cada 4 (quatro) meses.

Exemplos de composição de senhas que devem ser evitadas:

- Nome e sobrenome, especialmente os contidos no Login do Usuário;
- Números de documentos, matrículas funcionais, senhas bancárias ou de cartão de crédito, telefones, placas de carro ou datas que possam ser relacionadas ao usuário ou familiares;
- Palavras encontradas em dicionários;
- Palavras sugeridas a partir de objetos ou locais que possam ser vistos da mesa do Usuário;
- Palavras invertidas.

A senha não deve ser anotada em nenhum local - papéis, cadernos, post-its (ou similares) ou em qualquer material que as senhas possam ficar visíveis.

Não incluir senhas em processos automáticos de acesso ao sistema, mesmo que estes estejam disponíveis.

Não armazene senhas de acesso em equipamento pessoal.

Não utilize senhas de acesso à rede da Strata para fins pessoais

O usuário deve se certificar de que não está sendo observado ao digitar a sua senha.

A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial deve ser trocada pelo Usuário no primeiro acesso.

A solicitação de recuperação ou desbloqueio de senha deverá ser solicitada pelo próprio Usuário ao Suporte de TI (Help Desk). Ao receber uma nova senha, é responsabilidade do usuário alterar a senha temporária por uma definitiva na primeira utilização.

O Usuário que não efetuar acesso à rede corporativa em um período igual ou superior a 60 (sessenta) dias terá sua conta bloqueada

Caso o Usuário tenha 7 (sete) tentativas de acesso malsucedidas e consecutivas, sua conta será bloqueada por 30 (trinta) minutos.

O uso de acesso via VPN deverá ser restrito a usuários que necessitem de acesso à rede corporativa estando fora das localidades físicas de trabalho e para os usuários elegíveis à Política de Trabalho Híbrido – Home Office e Presencial.

5.7. Correio Eletrônico (E-mail)

O correio eletrônico é de propriedade da Strata e seu uso é permitido para as atividades profissionais dos usuários.

O uso particular do correio eletrônico é aceito desde que não prejudique o desenvolvimento das atividades profissionais.

O endereço de e-mail disponibilizado ao Usuário é de uso pessoal e intransferível, portanto, é terminantemente proibido modificar ou substituir a identidade do remetente ou destinatário de uma mensagem do correio eletrônico.

É vedado o uso de sistemas de webmail terceiros (Gmail, Hotmail, Yahoo, etc.) para fins profissionais. O uso do correio eletrônico para envio e recebimento de e-mail deverá ocorrer exclusivamente através do correio eletrônico da Strata, com extensão **@stratacapital.com.br**.

Os PST's das bases de e-mails não devem ser salvos nas estações de trabalho e nos servidores corporativos pelos Usuários

É proibido:

- a) enviar ou arquivar no servidor de e-mail mensagens contendo assuntos que provoquem perturbação ou assédio a outras pessoas ou que comprometam a

imagem do negócio da Strata perante seus clientes, fornecedores, clientes e comunidade em geral; temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético;

- b) cadastrar a conta de e-mail da Strata em qualquer tipo de site para fins particulares;
- c) efetuar configuração de e-mails pessoais nas estações de trabalho. Caso seja necessário o acesso aos e-mails pessoais através da Estação de Trabalho, este deve ser realizado através de webmail;
- d) executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou com características suspeitas. Em caso de dúvidas consulte o Help Desk;
- e) executar ou abrir links/endereços de e-mails suspeitos, como por exemplo bancos solicitando alguma informação pessoal. Verifique sempre se o e-mail ou endereço do link são realmente de fontes conhecidas. Em caso de dúvidas consulte o Help Desk;
- f) utilizar o e-mail corporativo para envio de grande quantidade de mensagens (spam) que possam comprometer a capacidade da rede, não reenviando e-mails do tipo corrente, materiais preconceituosos ou discriminatórios e os do tipo de boatos virtuais. Em caso de dúvidas consulte o Help Desk.

Usuários que possuem celulares corporativo do fabricante Samsung deverão possuir uma conta pessoal no Google com o objetivo de ativar e/ou atualizar serviços e/ou aplicativos destes celulares.

Anexos que contenham as extensões a seguir serão automaticamente bloqueados: .ace, .ani, .app, .docm, .exe, .jar, .reg, .scr, .vbe, .vbs, .bat, .cmd.

A disponibilização do correio eletrônico pode ser suspensa a qualquer momento por decisão do gestor da área do usuário ou da Gerência de Tecnologia.

As concessões e revogações de acesso ao serviço de correio eletrônico devem ser autorizadas pelo gestor da área do usuário e encaminhadas à Gerência de Tecnologia.

A utilização do correio eletrônico pode ser monitorada para fins de Segurança da Informação e nos processos de auditoria.

O monitoramento para fins disciplinares somente poderá ocorrer com a autorização do Comitê de Ética

Os Usuários devem evitar o envio de grandes volumes de anexos por e-mail (tamanho acima de 30 MB). Nestes casos, para o tráfego de grandes volumes de arquivos deve-se utilizar uma das alternativas a seguir:

- via diretório “Temporário” (transferência entre usuários com acesso à rede corporativa); ou
- através do OneDrive.

Não é permitida a alteração da assinatura de e-mail por parte dos Usuários. Tais assinaturas somente são alteradas através de solicitação formal da Gerência de Recursos Humanos.

As assinaturas dos e-mails de Colaboradores seguirão o padrão abaixo. Números de telefone fixo e celular (quando aplicável) serão informados, respectivamente, pelas áreas de TI e Administrativa:



Em caso de necessidade de acesso ao backup da base de e-mails (PST), o gestor responsável da área deve solicitar formalmente a Gerência de Tecnologia explicando o motivo pelo qual há necessidade de tal acesso:

- Próprio usuário – após análise da Gerência de Tecnologia, o PST poderá ser criado e disponibilizado somente ao próprio usuário;
- Outros usuários – após análise da Gerência de Tecnologia em conjunto com o Comitê da LGPD ou com Comitê de Ética, o PST poderá ser criado e disponibilizado ao Usuário designado pelo gestor, desde que exista justificativa que seja condizente com os interesses da Strata e sempre restrito à forma por esta autorizada, e, desde que o usuário designado pelo gestor assine o “TERMO DE RESPONSABILIDADE”, como consta no Anexo VI.

5.8. Acesso à Rede Corporativa

O acesso aos recursos da Rede Corporativa é realizado por meio do processo de Autenticação, utilizando as Credenciais de Acesso.

A licença para a utilização da Rede Corporativa é uma concessão da Strata aos Usuários que necessitam deste recurso para desempenhar suas funções. A utilização poderá ser monitorada e a licença suspensa a qualquer momento por decisão do gestor da área do Usuário ou da Gerência de Tecnologia.

Pasta Corporativa chamada “Temporário” tem o propósito de área de transferência e colaboração de arquivos temporários. Portanto, seu conteúdo é automaticamente excluído mensalmente, sem prévia comunicação.

É proibida a gravação de arquivos de uso pessoal nos diretórios corporativos “CORPORATE”, “PUBLICO” e “TEMPORARIO”. Tal gravação, se realmente necessária, deve ser realizada na respectiva Estação de Trabalho.

Caso seja necessária a criação de uma nova pasta (diretório) na Rede Corporativa (CORPORATE ou PUBLICO), o gestor responsável deve encaminhar um e-mail à Gerência de Tecnologia contendo as seguintes informações:

- Nome da nova Pasta Corporativa;
- Usuários que terão acesso à mesma;
- Tipo de acesso, por exemplo, somente leitura, leitura e edição, etc.

Os Colaboradores elegíveis à Política de Trabalho Híbrido – Home Office e Presencial automaticamente terão acesso remoto à rede corporativa (via VPN). Os Colaboradores não elegíveis precisam de autorização dos gestores para que tenham o acesso. Tais acessos remotos podem ser monitorados e bloqueados pela Gerência de Tecnologia ou por solicitação do respectivo gestor.

Diretores, gerentes e coordenadores têm acesso livre à VPN. Demais funcionários terão a VPN liberada de segunda à sexta-feira, das 08 às 20 horas. Exceções deverão ser aprovadas e controladas pelos gestores da área e Recursos Humanos.

É proibido o armazenamento de arquivos considerados improdutivos nos servidores da Strata, tais como, “Corporate”, “Público” e “Temporário”. São considerados arquivos improdutivos: filmes, fotos, músicas - excetuando-se os casos em que estes estejam diretamente relacionados às atividades do usuário, materiais contendo assuntos que provoquem perturbação ou assédio a outras pessoas ou que comprometam a imagem do negócio da Strata perante seus clientes, fornecedores, clientes e comunidade em geral; temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético. A Gerência de Tecnologia poderá remover tais arquivos sem anuência do Usuário.

Arquivos organizacionais devem ser salvos, preferencialmente, no “Corporate” ou “Público”, pois, arquivos gravados no computador (local) não possuem cópia de segurança (backup). É importante reforçar que não é de responsabilidade de TI a recuperação de arquivos que não respeitem as diretrizes desta Política de Confidencialidade e Segurança da Informação de .

Arquivos pessoais podem ser salvos no OneDrive. Em caso de dúvidas, favor procurar o Help Desk.

5.9. Acesso à Internet

A internet é um recurso corporativo disponibilizado aos Usuários para o desenvolvimento das atividades profissionais, enriquecimento intelectual ou como ferramenta de busca de informações, ou seja, tudo que possa vir a contribuir para o desenvolvimento das atividades relacionadas à Strata.

O acesso é monitorado pelo Diretor de Compliance.

A não ser quando indicado de forma diferente pelo gestor da área, todos os Usuários terão acesso à Internet.

O acesso à Internet para fins particulares é permitido desde que sejam respeitados os dispositivos legais e normativos vigentes, notadamente os estabelecidos nesta Política de Confidencialidade e Segurança da Informação. Tal uso não deve interferir no desempenho do próprio profissional ou de qualquer outro usuário, prejudicar o desempenho dos recursos disponíveis ou comprometer a imagem do negócio da Strata.

Os sites identificados como não seguros são automaticamente bloqueados. Ainda assim é responsabilidade do Usuário não acessar tais sites, dentre eles:

- Redes Sociais (exceto LinkedIn);
- Blogs, Sites de Chats e Páginas Pessoais;
- Streaming (exceto Spotify; Youtube);
- Conteúdo Adulto/Sexual Explícito;
- Jogos;
- Associações Criminosas, Preconceituosas, Extremistas, Armas, etc;
- Drogas e Alcool; e
- Pirataria.

Caso algum Usuário tenha necessidade de acessar algum site bloqueado pelo sistema, o gestor da área deverá formalizar tal solicitação, com justificativas, por e-mail à Gerência de Tecnologia.

É proibida a utilização de recursos que visem mascarar e/ou ocultar o tráfego de dados pela rede Strata, tais como serviços de Proxy ou de VPN's não autorizadas. A identificação da utilização deste tipo de recurso é passível de suspensão do direito do usuário de acessar a Internet nos ambientes corporativos.

5.10. Retenção de Dados

O gerenciamento do ciclo de vida das informações da Strata é vital para o bom desenvolvimento dos seus negócios.

Da criação até o descarte, as etapas do ciclo de vida das informações exigem planejamento e processos para garantir a continuidade do negócio e evitar a perda do conhecimento técnico.

Os detalhes sobre a retenção e descarte de dados pessoais podem ser consultados na Política de Privacidade e Proteção de Dados Pessoais.

5.11. Gestão de Incidentes

Implementamos medidas técnicas e organizacionais para proteger contra roubo, uso indevido e acesso, divulgação, alteração e destruição não autorizados.

Essas medidas incluem questões físicas, administrativas e eletrônicas (digitais) de segurança de acordo com a sensibilidade, quantidade, distribuição e formato das informações coletadas.

No entanto, sempre há um certo nível de risco envolvido quando as informações são coletadas, processadas e armazenadas, e, não é possível garantir a totalidade da segurança das informações. Em caso de incidente as etapas listadas abaixo deverão ser seguidas:

- a) Notificação interna – se qualquer incidente for identificado, seja por monitoramento automático, seja ativamente pelos Usuários ou por uma pessoa externa, o primeiro passo é registrar esse incidente através de um dos canais de comunicação constantes no item 17 abaixo;
- b) Notificação Externa – será realizada notificação em até 72 horas (setenta e duas) horas, diretamente na plataforma eletrônica SEI (Sistema Eletrônico de Informações) da Presidência da República (PR), em caso de vazamento de informações, conforme orientações da ANPD (Agência Nacional de Proteção de Dados). Os titulares de dados pessoais serão igualmente comunicados quanto ao problema, sendo o prazo contado a partir do momento de constatação do incidente.
- c) Usuário – é responsável por registrar o incidente através dos canais citados no item 17 abaixo ou pedir ajuda ao Help Desk; e
- d) Detecção Automática através de softwares e sistemas específicos.

Para qualquer registro relacionado a incidentes envolvendo “dados pessoais” será necessário incluir as pessoas responsáveis pela identificação do incidente e todos os detalhes adicionais sobre o assunto, buscando atender ao que disposto no art. 48 da LGPD, precisamente:

- a) descrição da natureza dos dados pessoais afetados;
- b) informações sobre os titulares envolvidos;
- c) indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, observados os segredos comercial e industrial;
- d) riscos relacionados ao incidente;
- e) motivos da demora, no caso de a comunicação não ter sido imediata; e
- f) medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A análise da criticidade será realizada pelo Comitê de LGPD com base em critérios específicos.

Atualizações periódicas sobre o tratamento do incidente serão realizadas interna e externamente.

Testes regulares serão realizados periodicamente para avaliar a eficiência relacionada aos requisitos de segurança e privacidade de dados pessoais.

A Strata classifica seus Incidentes de segurança da informação conforme a seguir:

Impacto	Significativo	• Severidade 1
	Médio	• Severidade 2
	Baixo	• Severidade 3

A classificação de impacto deve ser definida da seguinte maneira:

				
Classificação	Sistema	Informação	Recuperabilidade	Marca
Significativo	Os sistemas ou serviços com impacto significativo nos negócios estão inoperantes, comprometidos ou severamente degradados	Afeta dados confidenciais, sensíveis ou de alto risco que podem ter implicações significativas ao titular, considerações regulatórias significativas ou impacto significativo nas organizações ou indivíduos afetados	A recuperação do incidente é imprevisível e extremamente complexa	Alto impacto ou ameaça negativa grave à Strata, marca ou reputação mais ampla

Médio	Os sistemas ou serviços com impacto médio nos negócios ou clientes estão inoperantes, comprometidos ou severamente degradados	Afeta dados confidenciais que podem ter implicações no cliente e risco médio a baixo de danos às organizações ou indivíduos afetados	A recuperação do incidente pode ser imprevisível e complexa	Médio risco de impacto na marca ou imagem para Strata, clientes e parceiros
Baixo	Os sistemas ou serviços com impacto médio a baixo nos negócios estão inoperantes, comprometidos ou degradados	Somente informações públicas são afetadas e não têm implicações o cliente	A recuperação do incidente não é complexa, mas pode exigir coordenação com diferentes áreas da Strata	Baixo risco de impacto da marca ou imagem para Strata, clientes e parceiros

Tipos de Incidentes:

		
Tipo de Incidente	Descrição	Exemplo
Acesso não autorizado	Um indivíduo obtém acesso lógico ou físico sem permissão de uma rede, sistema, aplicativo, dados ou outro recurso da Strata	Ator desconhecido faz login na conta e um usuário remotamente
Denial of Service (DoS) – Negação de Serviço	Um ataque que impede ou prejudica com êxito a funcionalidade normal autorizada de redes, sistemas ou aplicativos, esgotando os	O site Strata é prejudicado por solicitações de conexões falsas de endereços IP maliciosos

	recursos. Essa atividade inclui ser a vítima ou participar do DoS	
Phishing	Mensagens personalizadas, com informações bem convincentes, com nome, sobrenome e outros dados, que levam o usuário a acreditar que está recebendo um e-mail legítimo de alguém familiar	O usuário recebe uma mensagem dizendo que seus dados precisam ser atualizados, pois a conta bancária pode ser desativada
Engenharia Social	Método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações	Abordagem via telefone para obter acesso não autorizado, seja se passando por um funcionário da empresa, fornecedor ou terceiros
Malware/Código Malicioso	É qualquer parte de um software que tenha sido codificada com o objetivo de danificar dispositivos, roubar dados e causar danos às pessoas, vírus, cavalos de Tróia, spywares e ransomwares estão entre os diferentes tipos de malwares	Arquivos são infectados por ransomwares, criptografando todo o conteúdo do disco, sendo possível acessá-los mediante o pagamento
Uso indevido / Mal uso dos sistemas	Uma pessoa viola a política de uso aceitável	Sistema possui softwares não autorizados
Uso indevido/ Mal uso dos sistemas	Uma pessoa viola a política de uso aceitável	Sistema possui softwares não autorizados
Scan/Probe/Tentativa de acesso	Qualquer atividade que procure acessar ou identificar um computador, portas abertas, protocolos, serviços ou outras ações para exploração posterior. Essa atividade nem sempre resulta em	O firewall externo da Strata está sendo “scaneado” por um IP externo suspeito para identificar portas abertas

	comprometimento ou negação do serviço	
Roubo e perda de notebook e celular corporativo	Equipamentos que são dedicados aos profissionais da STRATA CAPITAL que são roubados ou perdidos no período em que estão sob a guarda do profissional	Roubo de notebook e/ou celular corporativo em qualquer situação
Violação de políticas	Reúne um conjunto de diretrizes e boas práticas para o uso seguro das informações	Uso de softwares não permitidos
Vulnerabilidade técnica	Fraqueza que pode permitir a um atacante explorar um sistema a acessar informações não autorizadas	Ausência e patches de segurança do sistema operacional
Outros/ Investigação	Incidentes não confirmados que são potencialmente atividades maliciosas ou anômalas consideradas pela entidade que relata para solicitar uma revisão adicional	Suspeita de aumento de tráfego originado por um servidor

5.12. Proteção de Dados e Auditoria

Sistemas de TI e comunicação possuem registros de log que são gerados automaticamente. Esses logs são armazenados nas estações de trabalho e na rede, permitindo a detecção de erros, controle de acesso e atividades de Usuários.

Somente diretores, gestores, coordenadores ou demais Colaboradores expressamente autorizados por estes (mediante requerimento à Gerência de Automação e TIC) estão autorizados a utilizar pen drives nos micros e notebooks da Strata. Todos os micros e notebooks dos demais Colaboradores serão configurados para impedir o uso de tal dispositivo (pen drive). Tal ação visa, dentre outras, mitigar o risco de ataques de vírus.

Todos os dados e informações são protegidos por mais de uma camada de proteção.

5.13. Papéis e Responsabilidades

5.13.1. Todos os Usuários (funcionários, estagiários, prestadores de serviços):

- cumprir fielmente a Política de Confidencialidade e Segurança da Informação, bem como políticas e normas correlatas, como Política de Privacidade e Proteção de Dados Pessoais, Propriedade Intelectual, Compliance, etc;

- b) buscar orientação de gestores em caso de dúvidas relacionadas à Segurança da Informação;
- c) comunicar imediatamente eventuais casos de violação de Segurança da Informação, através da Gerência de Tecnologia, Comitê da LGPD ou Canal de Denúncias;
- d) proteger as informações contra acessos, modificações, destruição, divulgações não autorizadas
- e) responder pelo adequado uso dos ativos de TI que estiverem sob sua responsabilidade, de acordo com as diretrizes desta Política de Confidencialidade e Segurança da Informação e regras de patrimônio e Compliance;
- f) manter os arquivos de trabalho armazenados nos Servidores Corporativos (diretórios de rede);
- g) não salvar arquivos particulares nos servidores corporativos;
- h) relatar ao gestor imediato e à Gerência de Tecnologia sempre que identificar ou ocorrer dano, furto, roubo ou perda de um ativo de TI. Em caso de furto ou roubo será necessário apresentar o Registro de Ocorrência no órgão competente conforme previsto no “CONTRATO DE COMODATO”, como consta no Anexo V;
- i) responder pelas atividades que ocorram na sua conta de Usuário;
- j) manter sigilo quanto a senha de acesso aos recursos da rede corporativa;
- k) bloquear a Estação de Trabalho sempre que se afastar do equipamento, mesmo que esteja trabalhando em Home Office;
- l) desligar a Estação de Trabalho diariamente ao final do expediente;
- m) impedir o uso dos ativos de TI por outras pessoas, exceto em caso de reparo por pessoas autorizadas por TI;
- n) responder pelo uso adequado dos serviços e recursos disponibilizados com: Correio Eletrônico, sistemas, internet, etc;
- o) não armazenar dados corporativos em equipamento pessoal;
- p) não deixar documentos impressos na impressora e/ou copiadora, nem tampouco sobre as Estações de Trabalho;
- q) configurar o bloqueio do celular corporativo através de PIN, biometria ou senha.

5.13.2. Gestores:

- a) cumprir e fazer cumprir fielmente esta Política de Confidencialidade e Segurança da Informação, bem como políticas e normas correlatas, como Política de Privacidade e Proteção de Dados Pessoais, Propriedade Intelectual, Compliance etc.;
- b) assegurar que os membros de suas equipes tenham acesso e conhecimento desta Política de Confidencialidade e Segurança da Informação;
- c) comunicar imediatamente eventuais casos de violação de Segurança da Informação, através da Gerência de Tecnologia, Comitê da LGPD ou Canal de Denúncias;
- d) solicitar ou revogar solicitação junto à Gerência de Tecnologia quanto a disponibilização dos ativos de TI, acessos de rede corporativa, sistemas e internet necessários para o desempenho das funções dos usuários sob sua gestão;
- e) comunicar à Gerência de Tecnologia sempre que for necessário transferir a responsabilidade de um ativo de TI para um outro Usuário;
- f) informar imediatamente à Gerência de Tecnologia sobre os casos de inclusão, exclusão ou alteração de terceiros sob sua gestão;
- g) comunicar à Gerência de Tecnologia a ocorrência de direitos de acesso desnecessários dos Usuários sob sua gestão; e
- h) rever de forma periódica (não superior a 06 meses), o perfil de acesso em todos os sistemas (SAP, SGT, Portal de Agendamento, etc.) dos usuários sob sua gestão.

5.13.3. Gerência de Tecnologia:

- a) atualizar esta Política de Confidencialidade e Segurança da Informação, sempre que necessário;
- b) administrar os ativos de TI de forma a garantir a conformidade desta Política de Confidencialidade e Segurança da Informação;
- c) elaborar o contrato de comodato para entrega dos notebooks;
- d) garantir a ativação e desativação das contas, senhas e acessos de usuários por solicitação da Gerência de Recursos Humanos e/ou gestores;
- e) avaliar e tratar qualquer exceção relativa à esta Política de Confidencialidade e Segurança da Informação; e
- f) comunicar imediatamente à Diretoria Executiva sobre qualquer incidente relativo à Segurança da Informação.

5.13.4. Programa de Treinamento e Capacitação em Segurança da Informação: A Strata

manterá um programa permanente de treinamento e capacitação em segurança e sigilo das informações, em conformidade com o disposto no art. 24 da Resolução CVM 21.

O programa de treinamento deverá observar as seguintes disposições:

- a) participação obrigatória para todos os Colaboradores, administradores, membros de comitês estatutários e terceiros que tenham acesso a informações confidenciais ou participem, direta ou indiretamente, de processos de estruturação, distribuição ou gestão de títulos de securitização emitidos pela Strata;
- b) periodicidade anual, sem prejuízo da realização de sessões extraordinárias sempre que houver alterações normativas relevantes, modificações substanciais nesta Política de Confidencialidade e Segurança da Informação ou ocorrência de incidentes de descumprimento das diretrizes de segurança da informação, conforme previstas nesta Política de Confidencialidade e Segurança da Informação;
- c) novos Colaboradores devem participar do treinamento introdutório sobre esta Política de Confidencialidade e Segurança da Informação no prazo máximo de 30 (trinta) dias contados da data de início de suas atividades junto à Strata; e
- d) os treinamentos terão como conteúdo mínimo: (1) as diretrizes e procedimentos previstos nesta Política de Confidencialidade e Segurança da Informação; (2) identificação, classificação e tratamento de informações confidenciais; (3) procedimentos para prevenção e resposta a incidentes de segurança da informação; (4) uso adequado dos ativos de tecnologia da informação da Strata; (5) boas práticas de proteção de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018); e (7) sanções aplicáveis em caso de descumprimento das obrigações estabelecidas nesta Política de Confidencialidade e Segurança da Informação.

5.13.5. Gerência de Recursos Humanos:

- a) comunicar à Gerência de Tecnologia todos os casos de admissão, desligamentos, afastamentos e férias para que a área possa providenciar os acessos ou bloqueios necessários;
- b) comunicar à Gerência de Tecnologia as alterações de cargo, telefone, filial, etc., para os devidos ajustes de assinatura de e-mail e atualização de cadastro do outlook.

5.14. Violação da Política de Confidencialidade e Segurança da Informação

Toda e qualquer violação às diretrizes contempladas nesta Política de Confidencialidade e Segurança da Informação devem ser informadas à Gerência de Tecnologia.

Toda violação deverá ser investigada para determinação das medidas necessárias, visando a correção de falhas ou reestruturação do sistema.

Nota: Em caso de dúvidas quanto aos procedimentos e responsabilidades descritos nesta Política de Confidencialidade e Segurança da Informação, o Usuário ou gestor deverá entrar em contato com a Gerência de Tecnologia.

5.15. Boas Práticas

Cuidado ao tratar de assuntos da Strata dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega de trabalho, ou mesmo fornecedor/cliente.

Não é permitida a divulgação de nomes e tratativas de assuntos confidenciais.

Quando em deslocamentos de carro, coloque o notebook no porta-malas ou em local não visível.

Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para notebook e sim mochilas ou malas discretas. Não coloque o notebook em carrinhos de aeroportos e nem despache junto com a bagagem.

Em locais públicos mantenha sempre o notebook à vista, não se distanciando do equipamento.

Avalie se em pequenas viagens realmente é necessário levar o notebook.

Não conecte o equipamento em redes Wi-fi desconhecidas, essas redes podem conter mecanismos para captura de dados do seu dispositivo.

Documentos enviados para impressão devem ser retirados imediatamente das impressoras.

Documentos confidenciais não devem ficar expostos com fácil acesso, como por exemplo, sobre mesas.

5.16. Canais de Comunicação

Para esclarecimentos de dúvidas quanto a Política de Confidencialidade e Segurança da Informação ou para comunicação de eventuais incidentes de segurança, o canal abaixo deve ser acionado: tecnologia@stratacapital.com.br

6. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

Atualmente, a Strata desempenha atividades voltadas para (i) a gestão de carteiras de títulos e valores mobiliários, a qual é autorizada e exercida nos termos da Resolução CVM 21, e (ii) securitização, tais como aquelas previstas nas regulamentações específicas de securitização desde que não configurem atividade regulamentada privativa de companhia securitizadora junto à CVM.

Tais atividades exigem a segregação total de suas atividades de gestão de carteiras

administradas e de fundos de investimento, de securitização e de outras que futuramente possam vir a ser desenvolvidas pela Strata ou empresas controladoras, controladas, ligadas ou coligadas no âmbito do mercado de capitais, bem como prestadores de serviços.

Neste sentido, as equipes que desempenham atividades relacionadas à gestão de recursos e as equipes que desempenham atividades relacionadas à securitização são independentes e segregadas entre si, o que é assegurado por meio de acesso exclusivo por meio de ponto eletrônico, utilização de instalações físicas totalmente independentes e segregadas, disponibilização de linhas telefônicas específicas e diretório de rede privativo e restrito, acessível somente mediante login e senha individuais.

A Strata não contratará, num primeiro momento, terceiros para a prestação de serviços de back office e análise de valores mobiliários, contando apenas com seu departamento técnico para tanto.

No entanto, caso a Strata venha a contratar terceiros para a prestação de serviços de back office e análise de valores mobiliários, a Strata adotará regras e procedimentos internos capazes de assegurar a completa segregação de funções, atividades e responsabilidades relacionadas com a administração de carteira de valores mobiliários e com as operações de securitização, como aqueles previstos nos parágrafos acima.

A Strata poderá contratar, a qualquer momento, Terceiros que não estejam ligados à sua atividade principal.

Todos os Colaboradores deverão respeitar as regras e segregações estabelecidas nesta Política e guardar o mais completo e absoluto sigilo sobre as informações que venham a ter acesso em razão do exercício de suas atividades. Para tanto, cada Colaborador, ao firmar o Termo de Recebimento e Compromisso, anexo ao presente, atesta expressamente que está de acordo com as regras aqui estabelecidas e abstém-se de divulgar informações confidenciais que venha a ter acesso.

A Strata deve exercer suas atividades com lealdade e boa-fé em relação aos seus clientes, evitando práticas que possam ferir a relação fiduciária com eles mantida.

7. TRATAMENTO DE CONFLITO DE INTERESSES

Conflitos de interesses são situações decorrentes do desempenho das funções de determinado Colaborador, nas quais os interesses pessoais de tal Colaborador possam ser divergentes ou conflitantes com os interesses da Strata e/ou entre os interesses diferentes de dois ou mais de seus clientes, para quem a Strata tem um dever para cada um ("Conflito de Interesses").

O Colaborador tem o dever de agir com boa-fé e de acordo com os interesses dos investidores com o intuito de não ferir a relação fiduciária com o cliente. Para tal, o Colaborador deverá estar atento para uma possível situação de conflito de interesses, e sempre que tal situação ocorrer deverá informar, imediatamente, o Diretor de Compliance sobre sua existência e abster-se de consumir o ato ou omissão originador do Conflito de Interesses até decisão em contrário.

A Strata presta serviços de gestão discricionária de fundos de investimentos e de securitização.

A fim de evitar qualquer situação de potencial conflito de interesses entre as atividades de gestão e as atividades desempenhadas por sociedades em que os sócios e/ou diretores possuam participações societárias ou atuação funcional, é expressamente vedada a realização de qualquer tipo de investimento, direto ou indireto, em sociedades nas quais os sócios e/ou diretores possuam participações societárias ou atuação funcional, ressalvadas as hipóteses previstas no item 7.1 abaixo.

A Strata esclarece que a entidade da Strata que presta serviços de gestão discricionária de fundos de investimento possui sócios em comum com a entidade da Strata que presta serviços de securitização, situação que não configura infração às normas regulatórias aplicáveis, desde que observadas as regras de segregação de atividades e mitigação de conflitos de interesses previstas nesta Política, com ampla divulgação aos seus clientes sobre os potenciais conflitos de interesses, nos termos do item 7.2 abaixo.

Os sócios e/ou diretores e todos os funcionários estão obrigados a informar caso haja qualquer alteração no contexto acima descrito que possa gerar potencial conflito de interesses.

Ademais, a Strata destaca que toda e qualquer situação de potencial conflito de interesse será objeto de supervisão e controle específicos pelo Diretor de Compliance.

7.1. Operações entre Veículos de Investimentos e Empresas Relacionadas

Será permitida a realização de operações e negócios entre os veículos de investimentos geridos pela Strata e as empresas relacionadas a seus sócios indiretos e/ou diretores, desde que tais operações sejam conduzidas em estrita conformidade com a legislação aplicável, normas regulatórias e o presente Código, sendo observada a Política de Segregação das atividades, nos termos do item 6 acima.

7.2. Disclosure aos clientes

A Strata entende que a ampla divulgação de potenciais conflitos de interesses aos seus clientes é o meio mais eficaz de segregação de atividades e mitigação de conflitos de interesses. Portanto, quando do exercício de suas atividades, os Colaboradores devem atuar com a máxima lealdade e transparência com os clientes.

Isso significa, inclusive, que diante de uma situação de potencial conflito de interesses, a Strata deverá informar ao cliente que está agindo em conflito de interesses e as fontes desse conflito, mediante o envio de notificação eletrônica com aviso de recebimento.

8. POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO

8.1. Princípios Gerais

A prevenção da utilização dos ativos e sistemas da Strata para incorporação, na economia

do país, de modo permanente ou temporário, de recursos, bens e valores de origem ilícita (lavagem de dinheiro), ou para qualquer outra atividade ilegal, é dever de todos os Colaboradores e Terceiros da Strata, conforme determinado pelas legislações e regulações em vigor sobre Prevenção à Lavagem de Dinheiro e do Financiamento do Terrorismo (PLDFT) emitidas pelo Banco Central do Brasil e pela CVM; em especial a Lei nº 9.613/1998, conforme alterada pela Lei nº 12.683/2012 (“Lei de Lavagem de Dinheiro”), a Lei nº 13.260/2016, a Lei nº 13.810/19, a Circular 3.978, de 23 de janeiro de 2020 e Carta-Circular 4.001 de 29 de janeiro de 2020, ambas do Banco Central, e a Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada (“Resolução CVM 50”), bem como o Guia de Prevenção à “Lavagem de Dinheiro” e ao Financiamento do Terrorismo no Mercado de Capitais Brasileiro da ANBIMA.

O responsável perante a CVM pelo cumprimento de todas as normas aplicáveis, pela implementação dos mecanismos de controle delineados nesta Política de PLDFT, pelo treinamento dos colaboradores e por reportar qualquer atividade suspeita à CVM e ao Conselho de Controle de Atividades Financeiras (“COAF”) será o Diretor de Compliance.

Nos termos da Resolução CVM 50, a Strata deve, no limite de suas atribuições, identificar, analisar, compreender e mitigar os riscos de LD/FTP inerentes às suas atividades desempenhadas no mercado de valores mobiliários, adotando uma abordagem baseada em risco (“ABR”) para garantir que as medidas de prevenção e mitigação sejam proporcionais aos riscos identificados, assegurando cumprimento das regras aplicáveis. Desta forma, a Strata deverá, nos limites da sua atribuição, classificar em baixo, médio e alto risco de LD/FTP, observada as métricas descritas nesta Política, seus:

- a) Colaboradores;
- b) Serviços Prestados;
- c) Produtos Oferecidos;
- d) Cotistas;
- e) Prestadores de Serviços Relevantes; e
- f) Ativos.

A Strata, por meio do Diretor de Compliance, monitora a adequação dos critérios utilizados nesta Política para a definição e classificação da sua ABR, que foram elaboradas levando em conta a visão de outras áreas estratégicas, tais como área de Gestão, de Risco, Jurídico e de Securitização, além do embasamento em normas de PLD/FTP.

8.2. ABR

8.2.1. Colaboradores

O Diretor de Compliance realiza análise de *background check* de seus Colaboradores e potenciais colaboradores, com o intuito de prevenir situações de LD/FTP. Na referida análise será verificado o histórico do potencial colaborador, de forma a verificar se este possui ou já possuiu

envolvimento com crimes comuns, crimes financeiros, crimes ligados a LD/FTP ou outros delitos similares.

Caso seja identificado algum ponto relevante do ponto de vista de compliance, será levado de forma sigilosa ao Diretor de Compliance, que irá avaliar o caso e optar pela continuação ou não da contratação do potencial colaborador.

Como forma de manter os Colaboradores sempre atualizados com as normas de LD/FTP, são realizados treinamentos anuais de Compliance, que englobam especificamente o tema de PLD/FTP. Além disso, todos os Colaboradores, ao ingressarem no quadro de funcionários ou sócios da Strata, assinam e aderem ao Código de Ética da Strata e suas políticas, incluindo esta Política de PLDFT.

8.2.2. Serviços Prestados

Em relação aos serviços prestados, a Strata desenvolve as atividades de **(i)** administração de carteiras, na qualidade de gestor de recursos de terceiros, e **(ii)** de aquisição e vinculação a um patrimônio separado de direitos creditórios, com o objetivo de lastrear a emissão de valores mobiliários, tais como aqueles previstos nas regulamentações específicas de securitização desde que não configurem atividade regulamentada privativa de companhia securitizadora junto à CVM.

A Strata classifica os serviços por ela prestados, de maneira geral, como de “Baixo Risco” em relação à LD/FTP, tendo em vista os pontos elencados abaixo.

Em relação aos serviços relacionados à atividade de administração de carteiras, o “Baixo Risco” é justificado **(i)** a atividade de gestor de recursos de terceiros é altamente regulada pela CVM e pela ANBIMA; **(ii)** a Strata não distribui seus fundos; **(iii)** os Colaboradores são treinados, anualmente, inclusive no tocante a PLD/FTP; **(iv)** os Prestadores de Serviços Relevantes, conforme definido no item abaixo, são em sua maioria, registrados e supervisionados pela CVM, ANBIMA e BACEN, conforme o caso; e **(v)** a gestão de recursos de terceiros é realizada pela Strata de forma totalmente discricionária.

Em relação aos serviços relacionados à securitização, por sua vez, o “Baixo Risco” é justificado pelo conhecimento pela Strata das partes envolvidas nas operações de securitização em que realizada, com a realização de processo de Due Diligence para identificação de potenciais riscos e rastreabilidade de fluxos.

A forma de monitoramento dos serviços prestados pela Strata se dará conforme: a) acompanhamento constante da regulamentação e autorregulação em vigor aplicáveis à sua atividade, de forma a manter suas políticas internas e atuação sempre aderentes aos normativos vigentes; b) treinamento e preparo constante de seus Colaboradores, conforme definido nesta Política; e c) apresentação do relatório de controles internos, anualmente.

8.2.3. Produtos Oferecidos

Os Produtos Oferecidos pela Strata são Fundos de Investimento Financeiro (“FIFs” - Anexo I da Resolução CVM nº 175), Fundos de Investimento em Direitos Creditórios (“FIDCs” – Anexo II

da Resolução CVM nº 175), Fundos de Investimento em Participações (“FIPs” – Anexo IV da Resolução CVM nº 175), todos com gestão discricionária quanto à decisão de investimentos e desinvestimentos dos produtos, e ativos decorrentes de operações de securitização, com partes objetos de processos de Due Diligence pela Strata.

Adicionalmente, os cotistas da Strata são caracterizados como Investidores Profissionais a luz da regulamentação em vigor. Dessa forma, a Strata classifica os FIFs como de “Baixo Risco” em relação à LD/FTP e os FIDCs e FIPs como de “Médio Risco”. A Strata poderá atuar também com Fundos de Investimento Imobiliário (“FIIs” – Anexo III da resolução CVM nº 175), estes também serão considerados como de “Médio Risco” para fins dessa Política.

A forma de monitoramento dos produtos da Strata se dará conforme: a) acompanhamento constante da regulamentação e autorregulação em vigor aplicáveis aos seus produtos, de forma a manter suas políticas internas e atuação sempre aderentes aos normativos vigentes; b) treinamento e preparo constante de seus Colaboradores, conforme definido nesta Política; c) monitoramento dos Prestadores de Serviços Relevantes; e d) apresentação do relatório de controles internos, anualmente.

8.2.4. Cotistas

Nos termos da regulamentação e autorregulamentação aplicáveis, a responsabilidade primária pelo processo de identificação de Cotistas e dos procedimentos de Know Your Client (“KYC”) em fundos de investimento, com exceção dos fundos reservados/exclusivos, cabe ao respectivo intermediário ou distribuidor do fundo, conforme o caso, que deverá possuir políticas e procedimentos próprios de PLD/FTP. Sem prejuízo da responsabilidade da Strata pela análise dos Prestadores de Serviços Relevantes e pela análise, avaliação e monitoramento dos investimentos realizados pelo fundo de investimento, a Strata poderá, como melhores práticas, conduzir suas próprias diligências ou solicitar informações ao distribuidor acerca de cotistas pontuais, caso julgue necessário.

No tocante aos fundos reservados/exclusivos, estabelece-se uma presunção de que o gestor mantém com o Cotista relacionamento comercial direto. Mesmo diante dessa presunção, não compete ao gestor colher todas as informações cadastrais previstas no Anexo B à Resolução CVM 50, obrigação que recai sobre o distribuidor. Portanto, a Strata deverá apenas manter registro dessas informações conforme ABR, e conhecer o beneficiário final do cotista, até a pessoa natural. Além de elaborar diligências no distribuidor, nos termos abaixo, e poder solicitar informações sobre os Cotistas ao distribuidor, a qualquer tempo. Em caso de recusa, a Strata evidenciará sua tentativa e buscará obter as informações de que necessite junto com próprio Cotista ou por meio de fontes públicas confiáveis.

Ressalta-se que, de acordo com a Resolução CVM 50, considera-se como beneficiário final pessoa natural ou pessoas naturais que, isoladamente ou em conjunto, possuam, controlem ou influenciem significativamente, direta ou indiretamente, um cliente em nome do qual uma transação esteja sendo conduzida ou dela se beneficie.

8.2.5. Prestadores de Serviços Relevantes

No caso de prestadores de serviços relevantes contratados pela Strata, inclusive aqueles contratados pela Strata, na qualidade de gestora de fundos de investimento. (“Prestadores de Serviços Relevantes”), a Strata deverá classificá-los por grau de risco com o objetivo de destinar maior atenção àqueles que demonstrem maior probabilidade de apresentar envolvimento com LD/FTP.

Ressalta-se que, a Strata poderá contratar outros prestadores de serviços, ainda que não mencionados acima.

Para fins dessa Política serão considerados como Prestadores de Serviços Relevantes,

de Alto Risco, aqueles que:

- (i) não sejam cadastrados e regulados pela CVM, ANBIMA ou BACEN;
- (ii) não aceitem a inclusão de cláusula contratual relativa à declaração quanto ao cumprimento e aderência as políticas e procedimentos previstos na regulamentação e autorregulamentação no tocante a PLD/FTP;
- (iii) não possuam Diretor de Compliance;
- (iv) tenham sido julgados como culpados em processos sancionadores da CVM ou processos judiciais/administrativos nos últimos 5 (cinco) anos decorrentes de falhas na adoção de procedimentos de PLD/FTP entre outros crimes considerados relevantes pelo Diretor de Compliance; e
- (v) não tenham enviado o QDD ANBIMA, quando solicitado.

de Médio Risco, aqueles que:

- (i) tenham sido parte (porém sem que ainda tenha ocorrido julgamento) de processos sancionadores da CVM ou processos judiciais/administrativos nos últimos 5 (cinco) anos decorrentes de falhas na adoção de procedimentos de PLD/FTP e/ou processos que tenham sido indicados no Formulário de Referência, bem como demais crimes considerados relevantes pelo Diretor de Compliance;

de Baixo Risco, aqueles que:

- (i) não tenham sido enquadrados em qualquer dos itens acima.

Adicionalmente, a Strata irá verificar a estrutura da contratação destes Prestadores de Serviços Relevantes, bem como o método de pagamento, se são pouco usuais (pagamento em dinheiro, pagamento a outras entidades que não o Prestador de Serviço Relevantes, pagamento para contas mantidas em países diversos do país em que o Prestador de Serviço Relevantes está domiciliado ou onde os serviços são executados) ou fora do acordado.

Ademais, em razão da classificação de risco atribuída aos Prestadores de Serviços Relevantes, além da elaboração de relatórios de *background check* pelo Diretor de Compliance,

quando necessário, serão tomadas as medidas abaixo indicadas conforme periodicidade aplicável:

Alto Risco: O Diretor de Compliance deverá monitorar o Prestador de Serviços Relevantes, caso contrato, a cada 12 meses.

Médio Risco: O Diretor de Compliance deverá monitorar o Prestador de Serviços Relevantes, caso contrato, a cada 24 meses.

Baixo Risco: O Diretor de Compliance deverá monitorar o Prestador de Serviços Relevantes, caso contrato, a cada 36 meses.

Em todos os casos, a Strata deverá, periodicamente: (a) solicitar o QDD ANBIMA atualizado, quando aplicável; (b) realizar videoconferência ou reuniões in loco, quando necessário; (c) atualizar os relatórios de background check para os casos em que a Strata julgar pertinente; e (d) coletar informações e documentos societários atualizados.

8.2.6. Ativos

A Strata, no âmbito de suas atividades, entende que os mercados regulamentados de negociação de ativos, tais como a bolsa de valores e o mercado de balcão organizado, já oferecem adequados procedimentos para fins PLD/FTP. O tipo de emissão ou a forma de negociação do ativo das operações da Strata influenciam diretamente a classificação de risco de LD/FTP e seu monitoramento. Portanto, as situações elencadas a seguir, por se referirem a ativos sujeitos à observância de uma série de obrigações regulatórias, dispensam o gestor de recursos de diligências suplementares no que se refere a PLD/FTP, são elas:

- (i) ativos que tenham sido objeto de ofertas públicas iniciais e secundárias registradas de acordo com as normas emitidas pela CVM;
- (ii) ativos que tenham sido objeto de ofertas públicas com esforços restritos, dispensadas de registro de acordo com as normas emitidas pela CVM;
- (iii) ativos emitidos ou negociados por instituição financeira ou equiparada;
- (iv) ativos emitidos por emissores de valores mobiliários registrados na CVM; e
- (v) ativos de mesma natureza econômica dos listados acima, quando negociados no exterior, desde que (1) sejam admitidos à negociação em bolsas de valores, de mercadorias e futuros, ou (2) registrados em sistema de registro, custódia ou de liquidação financeira, devidamente autorizados em seus países de origem e supervisionados por autoridade local reconhecida pela CVM, ou (b) cuja existência tenha sido assegurada por terceiros devidamente autorizados para o exercício da atividade de custódia em países signatários do Tratado de Assunção ou em outras jurisdições, ou supervisionados por autoridade local reconhecida pela CVM.

Por outro lado, no caso de negociações privadas, a Strata entende haver um maior risco

de LD/FTP, razão pela qual atribui a necessidade de análise mais detalhada dos ativos que serão adquiridos pelos fundos da Gestora ("Operações Ativas"), incluindo a contraparte da operação, o emissor do ativo, os intermediários, consultores, escrituradores, custodiantes entre outros (denominados como "Agentes Envolvidos").

Com isso, nas negociações privadas, a Strata deverá proceder com o levantamento dos documentos e analisar as informações dos Agentes Envolvidos que sejam, no julgamento da Gestora, efetivamente relevantes para fins de PLD/FTP, levando em consideração que os prestadores de serviços mencionados seguirão as regras previstas no item E – Prestadores de Serviços Relevantes.

Quanto aos demais envolvidos, principalmente no tocante a contraparte e emissor do ativo, a Gestora seguirá uma análise detalhada, por meio de um processo fundamentalista, englobando entre outras, as particularidades do setor, estrutura societária, riscos jurídicos e reputacionais envolvidos entre outros.

Assim, com o objetivo de destinar maior atenção as operações negociadas de forma privada, a Strata classifica estas como Operações Ativas de Alto Risco. Portanto, estas são monitoradas, mensalmente. O monitoramento consistirá em atualizar as informações recebidas pela Strata, observando as obrigações contratuais impostas, bem como solicitar novas informações que essa vier a julgar pertinente.

Vale ressaltar que esse monitoramento se refere unicamente e exclusivamente a fins de PLD/FTP, visto que as operações também são monitoradas mensalmente pelo time de gestão, com finalidade distinta, mas, no entanto, possui obrigação de reportar quaisquer indícios de PLD/FTP, caso sejam identificados no monitoramento.

8.3. Comunicação COAF

As situações listadas abaixo podem configurar indícios da ocorrência dos crimes previstos na Lei nº 9.613, ou podem com eles relacionar-se, devendo ser analisadas com especial atenção e, devendo a Strata atribuir maior atenção no âmbito das suas operações para fins de manutenção e/ou alteração da classificação de ABR atribuída, bem como quanto à necessidade de providências adicionais junto às autoridades competentes:

- a) Realização de operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários para o fundo, ou de operações de securitização, que apresentem atipicidade em relação à atividade econômica do cliente ou incompatibilidade com a sua capacidade econômico-financeira;
- b) Resistência ao fornecimento de informações necessárias para o início de relacionamento ou para a atualização cadastral, oferecimento de informação falsa ou prestação de informação de difícil ou onerosa verificação;
- c) Apresentação de irregularidades relacionadas aos procedimentos de identificação e registro das operações exigidos pela regulamentação vigente;

- d) Solicitação de não observância ou atuação no sentido de induzir funcionários da instituição a não seguirem os procedimentos regulamentares ou formais para a realização de operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários para o fundo, ou de operações de securitização;
- e) Quaisquer operações ou conjunto de operações de compra ou de venda de ativos e valores mobiliários envolvendo pessoas relacionadas a atividades terroristas listadas pelo Conselho de Segurança das Nações Unidas;
- f) Realização de operações ou conjunto de operações de compra ou de venda de títulos e valores mobiliários, qualquer que seja o valor da aplicação, por pessoas que reconhecidamente tenham cometido ou intentado cometer atos terroristas, ou deles participado ou facilitado o seu cometimento;
- g) Quaisquer operações ou conjunto de operações de compra ou de venda de títulos e valores mobiliários com indícios de financiamento do terrorismo;
- h) Operações ou conjunto de operações de compra ou de venda de títulos e valores mobiliários fora dos padrões praticados no mercado;
- i) Realização de operações que resultem em elevados ganhos para os agentes intermediários, em desproporção com a natureza dos serviços efetivamente prestados;
- j) Operações nas quais haja deterioração do ativo sem fundamento econômico que a justifique;
- k) Operações com participação de contraparte da operação, o emissor do ativo, os intermediários, consultores, escrituradores, custodiantes entre outros ("Agentes Envolvidos"), pessoas naturais, jurídicas ou outras entidades que residam, tenham sede ou sejam constituídas, bem como com ativos de jurisdição offshore que: (i) Seja classificada por organismos internacionais, em especial o GAFI, como não cooperante ou com deficiências estratégicas, em relação à prevenção e ao combate à lavagem de dinheiro e ao financiamento do terrorismo; (ii) Com tributação favorecida e submetidos a regimes fiscais privilegiados, conforme normas emanadas pela Receita Federal do Brasil; (iii) Não possua órgão regulador do mercado de capitais, em especial, que tenha celebrado com a CVM acordo de cooperação mútua que permita o intercâmbio de informações financeiras de investidores, ou seja signatário do memorando multilateral de entendimento da OICV/IOSCO;
- l) Operações realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos Agentes Envolvidos;
- m) Operações que evidenciem oscilação significativa em relação ao volume ou frequência de negócios de qualquer dos Agentes Envolvidos;

- n) Operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos Agentes Envolvidos e beneficiários respectivos;
- o) Operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelos Agentes Envolvidos;
- p) Operações em que não seja possível identificar os beneficiários finais dos Agentes Envolvidos;
- q) Operações com transferências privadas de recursos e valores mobiliários sem motivação aparente e indícios de LD/FTP; e
- r) Agentes Envolvidos com relação aos quais existam notícias desabonadoras na mídia que tenham relevância para fins de LD/FTP.

Caso o Diretor de Compliance da Strata entenda pela existência da materialidade dos indícios existentes, será realizada a comunicação formal ao COAF, sob responsabilidade do Diretor de Compliance, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela a qual se refira a informação, no prazo de 24 (vinte e quatro) horas a contar da conclusão que, objetivamente, permita fazê-lo, todas as transações, ou propostas de transação, que possam ser consideradas como sérios indícios de crimes de LD/FTP, em que: (i) se verifiquem características excepcionais no que se refere às partes envolvidas, forma de realização ou instrumentos utilizados; ou (ii) falte, objetivamente, fundamento econômico ou legal.

Cada reporte deverá ser trabalhado individualmente, sendo que dele deverão constar, sempre que aplicável, as seguintes informações: (a) Data de início de relacionamento da Strata com pessoa autora ou envolvida na operação ou situação; (b) A explicação fundamentada dos sinais de alerta identificados; c) A descrição e o detalhamento das características das operações realizadas; (d) apresentação das informações obtidas por meio das diligências previstas nesta Política, inclusive informando tratar-se, ou não, de PEP, e que detalhem o comportamento da pessoa comunicada; e (e) a conclusão da análise, incluindo o relato fundamentado que caracterize os sinais de alerta identificados como uma situação suspeita a ser comunicada para o COAF, contendo minimamente as informações definidas nos itens acima.

Até o último dia do mês de janeiro de cada ano, desde que não tenha sido prestada ao longo do ano anterior nenhuma comunicação referente às transações ou propostas de transação que possam ser considerados indícios dos crimes de que ora se trata, deverá ser enviada à CVM uma declaração confirmando a não ocorrência de nenhuma transação passível de comunicação no ano civil anterior.

Todas as comunicações ao COAF ou, conforme o caso, a decisão pela não realização da comunicação, deverão ser arquivados pela Strata pelo prazo mínimo de 5 (cinco) anos contados da data do evento, comprometendo-se a Strata a observar a obrigação de confidencialidade acerca de tais informações.

Os Colaboradores devem guardar absoluto sigilo referente às comunicações efetuadas sobre LD/FTP e em hipótese alguma podem revelar ou dar ciência do ocorrido a outras pessoas que não o Diretor de Compliance.

8.4. Indicadores de Eficácia

A Strata realizará anualmente testes de aderência/eficácia das métricas adotadas, fazendo constar do relatório anual a respectiva conclusão, com base nos critérios abaixo:

- (i) Análise de Correspondência: das operações que tenham sido objeto de notificações, autuações ou comunicados provenientes de autoridades públicas e/ou órgãos e entidades de regulação e autorregulação que constatem indícios de atipicidades para fins de PLD/FTP, deverá ser definido em termos percentuais quantas foram objeto de avaliação prévia pela Strata em função de indício ou mera suspeita de prática de LD/FTP.
- (ii) Análise de Adequação: das operações que tenham sido objeto de comunicação pela Strata as autoridades públicas e/ou órgãos e entidades de regulação e autorregulação em função de indícios de atipicidades para fins de PLD/FTP, deverá ser definido em termos percentuais quantas foram consideradas materialmente relevantes por tais autoridades.
- (iii) Análise de Treinamento: percentual dos Colaboradores que compareceram aos treinamentos da Strata em relação ao total do quadro de Colaboradores.
- (iv) Análise de Rendimento: percentual correspondente à média total obtida pelos Colaboradores em eventuais testes relativos à PLD/FTP aplicados pela Strata.
- (v) Análise de Obrigações Regulatórias: percentual das situações em que a Strata tenha cumprido tempestivamente os prazos de detecção, análise e comunicações de atividades suspeitas previstos nesta Política.

As análises acima contarão com os seguintes percentuais de atendimento:

Indicador de Eficácia	% de Tempestividade
Alta	De 100 a 75
Adequada	De 75 a 50
Moderada	De 50 a 25
Baixa	De 25 a 0

8.4.1. Pessoas Politicamente Expostas

É considerada pessoa politicamente exposta, nos termos da Resolução 29/2017 do COAF e Resolução CVM 50, “aquela que desempenha ou tenha desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de seu

relacionamento próximo”.

A Strata tem o compromisso de conduzir investigações prévias e verificar as relações comerciais de qualquer contraparte de operações ou transações, com o propósito de identificar com antecedência a existência de pessoas politicamente expostas em qualquer negócio, e realizar procedimentos voltados para a identificação da origem dos recursos utilizados em quaisquer operações que envolvam pessoas identificadas como politicamente expostas.

A Strata ainda se compromete a supervisionar com mais rigor qualquer relação de negócios mantida com pessoas politicamente expostas, principalmente em caso de operações que envolvam não residentes politicamente expostos, sobretudo oriundos de países com os quais o Brasil possua relações financeiras e comerciais estreitas, ou proximidade étnica, linguística, política e/ou geográfica.

As **Pessoas Politicamente Expostas** (“**PEP**”) são aquelas:

- 1) Detentoras de mandatos eletivos dos Poderes Executivo e Legislativo da União;
- 2) Ocupantes de cargo, no Poder Executivo da União, de:
 - a) Ministro de Estado ou equiparado;
 - b) Natureza Especial ou equivalente;
 - c) Presidente, vice-presidente e diretor, ou equivalentes, de entidades da administração pública indireta; e
 - d) Grupo Direção e Assessoramento Superior - DAS, nível 6, ou equivalente;
- 3) Membros do Conselho Nacional de Justiça, do Supremo Tribunal Federal, dos Tribunais Superiores e dos Tribunais Regionais Federais, do Trabalho e Eleitorais;
- 4) Membros do Conselho Nacional do Ministério Público, o Procurador-Geral da República, o Vice-Procurador-Geral da República, o Procurador-Geral do Trabalho, o Procurador-Geral da Justiça Militar, Subprocuradores-Gerais da República e os Procuradores-Gerais de Justiça dos Estados e do Distrito Federal;
- 5) Membros do Tribunal de Contas da União e o Procurador-Geral do Ministério Público junto ao Tribunal de Contas da União;
- 6) Presidentes e tesoureiros nacionais, ou equivalentes, de partidos políticos;
- 7) Governadores e secretários de Estado e do Distrito Federal, os Deputados Estaduais e Distritais, os presidentes, ou equivalentes, de entidades da administração pública indireta estadual e distrital e os presidentes de Tribunais de Justiça, Militares, de Contas ou equivalente de Estado e do Distrito Federal; e
- 8) Os Prefeitos, Vereadores, Presidentes de Tribunais de Contas ou equivalente dos

Municípios.

Pessoas politicamente expostas no exterior

São também consideradas pessoas expostas politicamente aquelas que sejam no exterior:

- 1) Chefes de estado ou de governo;
- 2) Políticos de escalões superiores;
- 3) Ocupantes de cargos governamentais de escalões superiores;
- 4) Oficiais gerais e membros de escalões superiores do poder judiciário;
- 5) Executivos de escalões superiores de empresas públicas;
- 6) Dirigentes de partidos políticos; ou
- 7) Dirigentes de escalões superiores de entidades de direito internacional público ou privado.

Familiares e estreitos colaboradores de PEP

Também são relevantes as pessoas relacionadas às pessoas politicamente expostas:

FAMILIARES DE PEP: são considerados familiares os parentes, na linha direta, até o segundo grau; o cônjuge, o companheiro, a companheira; o enteado e a enteada.

ESTREITOS COLABORADORES DE PPE:

- (i) pessoas naturais que são conhecidas por terem sociedade ou propriedade conjunta em pessoas jurídicas de direito privado ou em arranjos sem personalidade jurídica, que figurem como mandatárias, ainda que por instrumento particular, ou possuam qualquer outro tipo de estreita relação de conhecimento público com uma PEP;
- (ii) pessoas naturais que têm o controle de pessoas jurídicas de direito privado ou em arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de uma PEP.

8.5. Avaliação Interna e Periódica de Risco

O Diretor de Compliance deve elaborar Relatório de Avaliação Interna de Risco de Lavagem de Dinheiro e Financiamento ao Terrorismo e a Proliferação de Armas de Destruição em Massa ("Relatório Interno" ou "AIR"), o qual será encaminhado para a alta administração (Comitê Executivo) até o último dia útil do mês de abril e referente ao ano anterior à data entrega.

9. POLÍTICA ANTICORRUPÇÃO

9.1. Introdução

A Strata está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, a Lei nº 12.846/13 e Decreto nº 8.420/15, a Lei de Improbidade Administrativa (Lei 8.429/92); a Lei de Lavagem de Dinheiro (Lei 9.613/1998 e Lei 12.683/2012); a Lei Brasileira Antitruste (Lei 8.884/1994 e Lei 12.529/2011), o United States Foreign Corrupt Practices Act (FCPA); o United Kingdom Bribery Act (UKBA); e as convenções internacionais de enfrentamento da Corrupção das quais o Brasil é signatário – em especial a Convenção sobre o Combate da Corrupção de Funcionários Públicos Estrangeiros em Transações Comerciais Internacionais (OCDE), Convenção Interamericana contra a Corrupção (OEA) e Convenção das Nações Unidas contra a Corrupção (ONU), aqui em conjunto denominadas como “Leis Anticorrupção”.

Qualquer violação desta Política de Anticorrupção e das Leis Anticorrupção pode resultar em penalidades civis e administrativas severas para a Strata e/ou seus Colaboradores e terceiros, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

9.2. Abrangência das Normas de Anticorrupção

As Leis Anticorrupção estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios, colaboradores e terceiros que atuem em seu nome ou benefício contra a administração pública, nacional ou estrangeira.

Considera-se agente público: todo aquele que exerce para o Poder Público, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função.

Considera-se administração pública estrangeira os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais.

As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).

Representantes de fundos de pensão públicos, cartorários e assessores de funcionários públicos também devem ser considerados “Agentes Públicos” para os propósitos desta Política de Anticorrupção e das Leis Anticorrupção.

9.3. Definição

Nos termos das Leis Anticorrupção, constituem atos lesivos contra a administração pública, nacional ou estrangeira, todos aqueles que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos:

- a) prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente

público, ou a terceira pessoa a ele relacionada;

- b) comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;
- c) comprovadamente utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;
- d) no tocante a licitações e contratos:
 - (i) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
 - (ii) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
 - (iii) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
 - (iv) fraudar licitação pública ou contrato dela decorrente;
 - (v) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
 - (vi) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
 - (vii) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.
 - (viii) dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

9.4. Normas de Conduta

É terminantemente proibido dar ou oferecer qualquer presente a agente público sem autorização prévia do Diretor de Compliance. Está vetado qualquer oferecimento ou promessa de valores ou “vale-presentes” a Agentes Públicos, sob pena de ser interpretado como “vantagem indevida” e, portanto, ser caracterizado como um ato de corrupção.

Os Colaboradores e terceiros que atuem em nome ou benefício da Strata deverão se atentar, ainda, que (i) qualquer valor oferecido a agentes públicos, por menor que seja, poderá caracterizar violação às Leis Anticorrupção e ensejar a aplicação das penalidades previstas; e (ii) a violação às Leis Anticorrupção estará configurada mesmo que a oferta de vantagem indevida

seja recusada pelo Agente Público.

Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou Agentes Públicos que não encontram previsão legal ou regulamentar.

Nenhum sócio ou Colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos. Qualquer ato que enseje a suspeita de violação às Leis Anticorrupção deverá ser imediatamente comunicado ao Diretor de Compliance para investigação e possível aplicação de medidas disciplinares.

10. VANTAGENS, BENEFÍCIOS E PRESENTES

10.1. Vantagens e Benefícios Proibidos

Os Colaboradores e os terceiros não devem, direta ou indiretamente, nem para si nem para terceiros, solicitar, aceitar ou admitir dinheiro, benefícios, entretenimento, favores, presentes, promessas ou quaisquer outras vantagens indevidas que possam influenciar o desempenho de suas funções ou como recompensa por ato ou omissão decorrente de seu trabalho.

Quaisquer presentes recebidos por um Colaborador, sejam eles ofertados por clientes, fornecedores, prestadores de serviços, parceiros de negócios ou outras entidades com as quais a Strata faz negócios, devem ser compartilhados com os demais Colaboradores ou, na impossibilidade da divisão, sorteados entre todos.

Os Colaboradores só poderão aceitar presentes, refeições ou outros benefícios sem prévia autorização do Diretor de Compliance nos seguintes casos:

- a) refeição que não possua qualquer objetivo de influenciar o bom desempenho das funções do Colaborador;
- b) não envolva Agente Público ou terceiro a ele relacionado;
- c) material publicitário ou promocional até um valor máximo de U\$D 100,00 (cem dólares) distribuídos no curso normal dos negócios;
- d) qualquer presente ou benefício com valor máximo de U\$D 100,00 (cem dólares) oferecido na ocasião excepcional de um aniversário ou outra ocasião semelhante, que não seja incomum e que não tenha qualquer intenção de influenciar indevidamente o Colaborador;
- e) qualquer presente ou benefício com máximo de U\$D 100,00 (cem dólares); e
- f) presente da família ou amigos não ligados a deveres e responsabilidades profissionais e não relacionados a qualquer Agente Público.

Caso o benefício ou presente não se enquadre nos dispostos acima, o Colaborador só

poderá aceitá-lo mediante prévia autorização do Diretor de Compliance . Sempre que houver dúvida sobre a aceitação de determinado item, o Diretor de Compliance deverá ser previamente consultado.

Soft Dollar

Em termos gerais, *Soft Dollar* pode ser definido como sendo o benefício econômico (não-monetário) concedido à Strata por corretoras de títulos e valores mobiliários ou outros fornecedores (“Fornecedores”) na forma de pesquisas e outras formas de auxílio no processo de tomada de decisões de investimento em contraprestação ao direcionamento de transações dos fundos de investimento e carteiras administradas geridos pela Strata.

Tais benefícios serão utilizados pelos Colaboradores exclusivamente para fins de tomada de decisões de investimento e suporte à gestão dos fundos de investimento geridos pela Strata. A Strata não selecionará seus Fornecedores considerando somente os benefícios recebidos por meio de acordos de *Soft Dollar*, mas levará em consideração, primordialmente, a qualidade, eficiência, produtividade e os custos oferecidos por tais Fornecedores.

A Strata, por meio de seus representantes, deverá observar os seguintes princípios e regras de conduta ao firmar acordos de *Soft Dollar*.

- a) colocar os interesses dos clientes acima de seus próprios interesses;
- b) definir de boa-fé se os valores pagos pelos clientes e, consequentemente, repassados aos Fornecedores, são razoáveis em relação aos serviços de execução de ordens;
- c) ter a certeza de que o benefício *Soft Dollar* auxiliará diretamente no processo de tomada de decisões de investimento e alocar os custos do serviço recebido de acordo com seu uso, se o benefício apresentar natureza mista;
- d) divulgar amplamente a clientes, potenciais clientes e ao mercado, os critérios e políticas adotadas com relação às práticas de *Soft Dollar*, bem como os potenciais conflitos de interesses oriundos da adoção de tais práticas;
- e) cumprir com seu dever de lealdade, transparência e fidúcia com os clientes; e
- f) transferir à carteira dos clientes qualquer benefício ou vantagem que possa alcançar em decorrência de sua condição de gestora de carteira de valores mobiliários, conforme disposto no Artigo 16, inciso VI da Resolução CVM 21.

Os acordos de *Soft Dollar* devem ser transparentes e mantidos por documento escrito. A Strata deverá manter registros dos benefícios recebidos, identificando, se possível, a capacidade de contribuírem diretamente para o processo de tomada de decisões de investimento, visando comprovar o racional que levou a firmar tais acordos de *Soft Dollar*.

Ao contratar os serviços de execução de ordens, a Strata não buscará somente o menor custo, mas o melhor custo-benefício, em linha com os critérios de *best execution* estabelecidos no mercado internacional, devendo ser capaz de justificar e comprovar que os valores pagos aos

Fornecedores com que tenha contratado *Soft Dollar* são favoráveis aos fundos de investimento e carteiras administradas sob sua gestão comparativamente a outros Fornecedores, considerados para tanto não apenas os custos aplicáveis, mas também a qualidade dos serviços oferecidos, que compreendem maior eficiência na execução de transações, condições de segurança, melhores plataformas de negociação, atendimento diferenciado, provimento de serviço de análise de ações e qualidade técnica dos materiais correspondentes, disponibilização de sistemas de informação, entre outros.

Quaisquer benefícios não relacionados ao processo de tomada de decisão de investimentos, tais como pagamento de despesas de escritório, viagens, entretenimento, entre outros, não devem ser objeto de *Soft Dollar*.

Os acordos de *Soft Dollar* não devem gerar qualquer vínculo de exclusividade ou de obrigação de execução de volume mínimo de transações os Fornecedores, devendo a Strata manter atodo tempo total independência para selecionar e executar com quaisquer Fornecedores operações em nome dos fundos de investimento sob gestão e carteiras sob sua administração, sempre de acordo as melhores condições para seus clientes.

11. PROGRAMA DE TREINAMENTO

Todos os Colaboradores e Terceiros selecionados pelo Diretor de Compliance, ao serem contratados, deverão aderir a esta Política, bem como participar de um treinamento ministrado pelo Diretor de Compliance, que abrangerá:

- a) Discussão sobre todos os temas desta Política, inclusive consequências decorrentes do descumprimento;
- b) Apresentação das regras de segurança e confidencialidade das informações de clientes, investidores e carteiras dos fundos de investimentos geridos pela Strata, delineadas na Política de Confidencialidade e Segurança da Informação contida nesta Política;
- c) Discussão das regras sobre comunicação com terceiros e com a imprensa, conforme as determinações do Manual de Conduta e Ética;
- d) Discussão sobre as regras de negociação de títulos e valores mobiliários pelos colaboradores, conforme as determinações da Política de Compra e Venda de Valores Mobiliários da Strata;
- e) Discussão acerca das situações que podem configurar conflitos de interesse;
- f) Discussão sobre as regras de diferentes órgãos reguladores que impactem os negócios da Strata;
- g) Discussão sobre as eventuais certificações necessárias para o desempenho das funções; e
- h) Temas para prevenção de crime de lavagem de dinheiro e financiamento ao

terrorismo.

Adicionalmente, todos os Colaboradores serão convocados anualmente, ou em frequência menor se assim avaliado pelo Diretor de Compliance, a participar de atualizações periódicas desta Política através de treinamento ministrados pelo Diretor de Compliance.

Todos os Colaboradores e terceiros selecionados pelo Diretor de Compliance deverão declarar que passaram por treinamento com a devida instrução sobre a Política, tanto na contratação quanto na atualização anual.

12. PENALIDADES PARA DESVIOS DE CONDUTA DOS COLABORADORES

O descumprimento total ou parcial das determinações contidas nos Manuais e Políticas da Strata e na legislação vigente constitui violação dos padrões que regem o funcionamento da Strata, e acarretará a abertura de investigação interna para apuração de possíveis desvios de conduta.

Caso o desvio se confirme, serão aplicadas sanções que podem resultar em (i) aplicação de advertência, (ii) suspensão, ou (iii) demissão, conforme a avaliação realizada pelo Diretor de Compliance e conforme a gravidade do ato praticado. Ao Terceiro infrator, poderão ser aplicadas penalidades previstas em contrato, inclusive a sua rescisão.

Caso o desvio de conduta seja praticado por um dos membros do Comitê Executivo, tal membro não poderá participar do processo de avaliação de conduta e definição da sanção a ser tomada.

Quaisquer penalidades poderão ser aplicadas a qualquer Colaborador ou terceiro que viole as disposições dos Manuais e Políticas da Strata, sem prejuízo das responsabilidades civis e criminais estabelecidas em lei, conforme aplicável. Os Colaboradores que não comunicarem eventuais violações ou omitirem informações relevantes também estarão sujeitos às sanções disciplinares e legais acima mencionadas.

A aplicação de sanções disciplinares não impede a adoção de medidas legais cabíveis, para reparar eventuais danos provocados pelos Colaboradores à Strata.

Não haverá nenhuma retaliação ao Colaborador ou ao terceiro que, de boa-fé, comunique qualquer suspeita de violação ao Programa de Compliance da Strata, ainda que posteriormente seja verificado que o fato não ocorreu. A Strata apoia totalmente o reporte de condutas possivelmente indevidas ao Diretor de Compliance. Contamos com acolaboração de todos!

Controle de Revisões

Data da última revisão: Junho de 2026.

ANEXO I

DEFINIÇÕES DA POLÍTICA DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

AMBIENTE FÍSICO: engloba os ativos da empresa, como instalações e equipamentos.

AMBIENTE LÓGICO: conjunto de sistemas, dados e programas da empresa.

ANPD: a Autoridade Nacional de Proteção de Dados.

ANTISPAM: ferramenta utilizada para bloquear mensagens indesejadas de correio eletrônico (Spams).

ATIVOS DE TIC: estações de trabalho (Desktop/Notebook), celulares, servidores, softwares, arquivos, correio eletrônico, dispositivos de autenticação e quaisquer equipamentos eletrônicos ou sistemas relacionados à tecnologia da informação e comunicação.

AUTENTICAÇÃO: processo de verificação da identidade de um usuário ou sistema, necessário para autorizar a utilização de recursos corporativos de TIC e ao acesso das informações de propriedade da Strata. Tal processo tem como objetivo confirmar a identidade do usuário ou entidade que está tentando acessar a informação.

BACKUP: cópia de dados ou arquivos digitais, de um dispositivo de armazenamento para outro, de forma que os dados ou o sistema possa ser restaurado em caso de perda dos dados originais.

CATÁLOGO DE ENDEREÇOS: agenda de endereços eletrônicos existente na aplicação de correio eletrônico.

CONFIDENCIALIDADE: garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada; princípio cujo objetivo é limitar o acesso à informação tão somente a pessoas, entidades e processos autorizados pelo titular da informação.

CONTA DE USUÁRIO: credencial de Acesso aos Recursos da Rede Corporativa que identifica o usuário que a utiliza. Seu uso é pessoal, intransferível e de responsabilidade do próprio Usuário. É identificado pelo termo “Login” nos Recursos da Rede Corporativa.

CRIPTOGRAFIA: mecanismo com objetivo de impedir que as informações trocadas sejam lidas indevidamente por pessoas não autorizadas.

DATA CENTER: ambiente projetado para abrigar equipamentos de TI (servidores, firewalls, etc.). O objetivo principal de um Data Center é garantir a alta disponibilidade dos sistemas hospedados.

DISPONIBILIDADE: princípio cujo objetivo é garantir que a informação esteja sempre acessível e utilizável pelas pessoas, entidades e processos autorizados, sempre que estes necessitarem.

DISPOSITIVOS DE ARMAZENAMENTO MÓVEL: incluem, entre outros, pen-drive, disco removível, CD, DVD e HD externo.

E-MAIL: forma reduzida para E(lectronic)-Mail - Correio Eletrônico.

ESTAÇÃO DE TRABALHO: computador (Desktop ou notebook) e seus periféricos que o Usuário utiliza para exercer suas atividades profissionais.

INCIDENTE DE SEGURANÇA: um ou mais eventos indesejados ou inesperados, que tenham uma probabilidade de acarretar riscos ou danos a direitos dos titulares, comprometendo as operações do negócio e/ou ameaçando a Segurança da Informação e/ou permitindo acesso indevido ou ilícito sem o consentimento do titular de dados.

INTEGRIDADE: propriedade de salvaguarda da exatidão e completeza da informação mantendo todas as características originais estabelecidas pelo proprietário da mesma; princípio que tem como objetivo garantir que apenas pessoas, entidades e processos autorizados possam alterar o conteúdo das informações corporativas.

INTERNET: sistema global de rede de computadores interligados através de um conjunto padrão de protocolos.

LGPD: Lei 13.709/18 – Lei Geral de Proteção de Dados pessoais.

LOG: termo técnico para descrever o registro das transações que ocorrem quando um software é utilizado.

ONEDRIVE: serviço de armazenamento na nuvem da Microsoft.

PHISHING: corresponde a “pescaria”, tem por objetivo “pescar” informações e dados pessoais importantes através de mensagens falsas. Com isso, os criminosos podem conseguir nomes de usuários, senhas e dados pessoais de um site qualquer, como também são capazes de obter dados de contas bancárias e cartões de crédito.

PST: arquivo de dados do Outlook que contém mensagens e outros itens do Outlook de uma determinada conta, o qual é salvo no computador.

RECURSOS DA REDE CORPORATIVA: consistem em todas as Pastas Corporativas, serviços, sistemas e equipamentos de Tecnologia da Informação da Strata.

SEGURANÇA DA INFORMAÇÃO: está diretamente relacionada com a proteção de um conjunto de informações de ativos de informação, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

SOFTWARE: é a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

SOFTWARES HOMOLOGADOS: softwares habilitados para funcionamento no Ambiente de Automação e TI da STRATA CAPITAL, testados e aprovados previamente pela Gerência de Tecnologia.

SOFTWARES LICENCIADOS: softwares para os quais tenham sido adquiridas Licenças de Uso fornecidas pelos seus respectivos fabricantes.

SPAM: mensagem não solicitada, normalmente indesejada, enviada para um grande número de pessoas.

TA: Tecnologia da Automação.

TIC: Tecnologia da Informação e Comunicação.

USB: é um tipo de conexão em computadores que permite a comunicação entre computadores e mídias removíveis de armazenamento de dados ou periféricos (teclado, mouse, etc).

USUÁRIO: qualquer Colaborador da Strata que utiliza algum serviço de informação disponibilizado pela Strata na execução de suas funções

VPN (VIRTUAL PRIVATE NETWORK OU REDE VIRTUAL PRIVADA): é uma forma de comunicação segura entre redes privadas através da Internet.

ANEXO II

TERMO DE RECEBIMENTO E COMPROMISSO DA POLÍTICA DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS DA STRATA

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____, DECLARO para os devidos fins:

(I) Ter recebido, na presente data, a Política de Regras, Procedimentos e Controles Internos atualizada (“Política”), incluindo a Política de Confidencialidade e Segurança da Informação e a Política de PLDFT, das empresas do Grupo Strata (“Strata”);

(II) Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes na Política, inclusive a respeito do tratamento a ser dado às informações confidenciais e privilegiadas;

(III) Estar ciente de que a Política como um todo passa a fazer parte dos meus deveres como Colaborador da Strata, incorporando-se às demais regras internas adotadas pela Strata; e

(IV) Estar ciente do meu compromisso de comunicar ao Diretor de Compliance da Strata qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas nesta Política.

[•], [•] de [•] de [•].

[COLABORADOR]

ANEXO III
PRINCIPAIS NORMATIVOS APLICÁVEIS

1. Resolução CVM 21, de 25 de fevereiro de 2021, conforme alterada;
2. Resolução CVM 175, de 23 de dezembro de 2022, conforme alterada;
3. Resolução CVM 50, de 31 de agosto de 2021, conforme alterada;
4. Guia de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo no Mercado de Capitais Brasileiro, elaborado pela ANBIMA
5. Código ANBIMA de Administração e Gestão de Recursos de Terceiros; e
6. Leis Anticorrupção.

ANEXO IV
TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº _____ (“Colaborador”), DECLARO para os devidos fins:

- (i) que a disponibilização pelo Colaborador às empresas do Grupo Strata (“Strata”), nesta data, dos documentos contidos no *pen drive* da marca [•], número de série [•] (“Documentos”), bem como sua futura utilização pela Strata, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;
- (ii) ciência e concordância de que quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, nos Documentos, serão de propriedade exclusiva da Strata, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Strata, exceto se aprovado expressamente pela Strata.

Para os devidos fins, o Colaborador atesta que os Documentos foram duplicados no *pen drive* da marca [•], número de série [•], que ficará com a Strata e cujo conteúdo é idêntico ao *pendrive* disponibilizado pelo Colaborador.

Os *pen drives* fazem parte integrante do presente termo, para todos os fins e efeitos de direito. A lista de arquivos constantes dos *pen drives* se encontra no Apêndice ao presente termo.

[•], [•] de [•] de [•].

[COLABORADOR]

ANEXO V
TERMO DE CIÊNCIA DE MONITORAMENTO

Por meio deste instrumento eu, _____, inscrito no CPF sob o nº ____ (“Colaborador”),
DECLARO para os devidos fins que tenho ciência e concordo que as empresas do Grupo Strata,
poderão acessar os dispositivos corporativos (ex.: notebook, celular, tablets etc.) que me forem
confiados para o exercício de minhas atividades.

[•], [•] de [•] de [•].

[COLABORADOR]

ANEXO VI
CONTRATO DE COMODATO

COMODANTE:

STRATA CAPITAL GESTÃO DE RECURSOS LTDA., com Sede na Rua Iguatemi, 192, conjuntto173 – Itaim Bibi – CEP: 001451-010 – São Paulo/SP, inscrita no CNPJ/MF sob o nº 43.179.785/0001-14, neste ato representada por seu procurador Sr(a). (nome), (nacionalidade), (Estado Civil), (Cargo), portador da carteira de identidade nº xxxxx (órgão emissor), C.P.F. nº xxx.xxx.xxx-xx, com endereço comercial na sede da empresa, na forma do Contrato Social da STRATA CAPITAL;

COMODATÁRIO: (nome completo do usuário), nacionalidade, Estado Civil, Cargo, portador da Carteira de Identidade nº XXXXXXXXXXXXXXXX, C.P.F. sob o nº xxx.xxx.xxx-xx, e, com endereço comercial na Rua xxxxxxxxxxxx.

As Partes acima identificadas têm, entre si, justo e acertado o presente Contrato de Comodato de Equipamentos de TI, doravante denominado simplesmente CONTRATO, que se regerá pelas cláusulas seguintes e pelas condições descritas no presente.

Cláusula 1ª. O presente contrato tem como OBJETO, a transferência, pela COMODANTE ao COMODATÁRIO, dos direitos de uso e gozo dos Equipamentos descritos a seguir, por prazo indeterminado:

- (descrição dos equipamentos, com marca, modelo, número série, cor, etc)
- Cláusula 2ª. Os Equipamentos, objeto deste CONTRATO, serão utilizados, prioritariamente, no desempenho das funções profissionais do COMODATÁRIO.

Cláusula 3ª. O COMODATÁRIO está obrigado a comunicar imediatamente à COMODANTE eventuais defeitos encontrados nos Equipamentos e disponibilizá-los para conserto, bem como a apresentar Registro de Ocorrência na hipótese de furto ou roubo do Equipamento.

Cláusula 4ª. O COMODATÁRIO se obriga, ainda, que no caso de quebra, dano integral ou parcial, decorrente de mau uso, que impeça ou limite a utilização dos Equipamentos, roubo ou furto (sem apresentação do Registro de Ocorrência), perda etc., a reembolsar o valor equivalente ao Equipamento, conforme Nota Fiscal do produto, em até 30 (trinta) dias, podendo, inclusive, ser utilizado o desconto em folha.

Cláusula 5ª. O COMODATÁRIO declara que recebe o equipamento em perfeito estado de conservação e funcionamento e se compromete de outro lado, a não só conservá-lo e guardá-lo, como igualmente a vigiá-lo, como FIEL DEPOSITÁRIO do mesmo, como ora nomeado.

Cláusula 6ª. O COMODATÁRIO deverá devolver o equipamento à COMODANTE sempre que for solicitado, a qualquer tempo e independente do término ou da rescisão do contrato de trabalho e no idêntico estado em que foi entregue.

Por estarem assim justos e contratados, firmam o presente instrumento, em duas vias de igual teor, juntamente com 2 (duas) testemunhas.

Local, data. _____

COMODANTE

COMODATÁRIO

Testemunhas: _____ Nome:

Nome: CPF:

ANEXO VII**TERMO DE RESPONSABILIDADE PARA ACESSO DE E-MAILS DE TERCEIROS**

Eu, [NOME COMPLETO], [qualificação], inscrito(a) no CPF sob nº [completar], na qualidade de usuário, declaro estar ciente e comprometido em observar e cumprir todas as diretrizes, normas e procedimentos das empresas do Grupo Strata no decorrer do acesso e uso da base de e-mails do ex-usuário xxxx (e-mail: xxxx@stratacapital.com.br), cujo conteúdo fica disponível para meu conhecimento e que eventualmente possa conter dados pessoais do ex-usuário ou de terceiros.

Estou ciente ainda de que:

- a) qualquer ativo (inclusive os de Tecnologia da Informação) que acesse, armazene, transforme ou transporte informações que se definam como dado pessoal, identificando ou tornando uma pessoa física identificável, deverá ser condizente com os interesses da Strata e na forma por esta autorizada;
- b) a Política de Segurança da Informação prevê o monitoramento dos e-mails corporativos, e se me deparar com dados pessoais de terceiros ao utilizar o e-mail corporativo, tal uso e monitoramento deve atender aos objetivos determinados pela Strata, e ser impessoal e sem discriminação observando as normas impostas pela LGPD – Lei 13.709/18 – Lei Geral de Proteção de Dados Pessoais;
- c) qualquer pesquisa que seja feita em e-mails corporativos deverá ser procedida exclusivamente para a finalidade determinada pela Strata e que, caso me depare com dados pessoais, incluindo dados pessoais sensíveis, não vou salvar, utilizar, acessar, reproduzir, transmitir, ou proceder com qualquer outro tipo de tratamento desses dados pessoais em discordância das regras para proteção dos mesmos;
- d) qualquer infração ao exato e pontual cumprimento de quaisquer das condições descritas neste Termo e nos documentos relacionados, por minha ação ou omissão, constituirá infração e poderá caracterizar condição para encerramento justificado do meu contrato de trabalho ou de prestação de serviços. Reconheço que este Termo passa a integrar respectivamente meu contrato de trabalho ou prestação de serviço;

Sendo assim, me responsabilizo por adotar as medidas de segurança estabelecidas nas políticas internas da Strata, incluindo a Política de Segurança da Informação e a Política de Privacidade e Proteção de Dados, buscando proteger dados pessoais de quaisquer Titulares eventualmente identificados em e-mails corporativos, devendo comunicar imediatamente à Gerência de Tecnologia qualquer incidente de segurança que possa acarretar risco ou dano relevante, conforme prevê a LGPD.

Local e data / Nome por extenso e assinatura /CPF: