STRATEGI CAPITAL GESTÃO DE RECURSOS LTDA.

POLÍTICA DE SEGREGAÇÃO, CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Agosto/2020

Strategi Capital

ÍNDICE

1. INTRODUÇÃO E OBJETIVO

A presente política de segregação, confidencialidade, segurança da informação e segurança cibernética da **STRATEGI CAPITAL GESTÃO DE RECURSOS LTDA.** ("STRATEGI CAPITAL" ou "GESTORA") tem por objetivo descrever os procedimentos observados pela GESTORA para garantir a devida segregação, confidencialidade e segurança das informações e cibernética, para fins de atendimento ao disposto na regulamentação vigente, bem como abordar o plano de contingência e continuidade dos negócios da STRATEGI CAPITAL.

Esta política de segregação, confidencialidade, segurança da informação e segurança cibernética se aplica aos sócios, administradores, funcionários e todos que, de alguma forma, auxiliam o desenvolvimento das atividades da STRATEGI CAPITAL ("Colaboradores").

2. POLÍTICA DE CONFIDENCIALIDADE

2.1. Confidencialidade e Conduta

As disposições da presente seção se aplicam aos Colaboradores que, por meio de suas funções na GESTORA, possam ter ou vir a ter acesso a informações confidenciais, reservadas ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

Todos os Colaboradores deverão ler atentamente e entender o disposto neste documento, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no Anexo II ao manual de regras, procedimentos e controles internos da STRATEGI CAPITAL ("Termo de Confidencialidade").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora da GESTORA. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais (especialmente, mas não de forma limitada, aquelas indicadas no Anexo III do manual de regras, procedimentos e controles internos da STRATEGI CAPITAL) e de compliance da GESTORA.

São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste documento, independente destas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou

intangível, qualquer informação sobre a GESTORA, sobre as empresas pertencentes ao seu conglomerado, se houver, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da STRATEGI CAPITAL , incluindo:

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

(ii) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela GESTORA;

(iii) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela GESTORA;

(iv) Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;

(v) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da GESTORA e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da GESTORA e que ainda não foi devidamente levado à público;

(vi) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;

(vii) Transações realizadas e que ainda não tenham sido divulgadas publicamente, bem como informações que não tenham sido tornadas públicas, mesmo com a divulgação da operação que integram; e

(viii) Outras informações obtidas junto a sócios, diretores, funcionários, trainees, estagiários ou jovens aprendizes da GESTORA ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados. A revelação de Informações

Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente informada ao Diretor de Compliance, Risco e PLDFT, conforme definido no contrato social vigente da STRATEGI CAPITAL, para que esta decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Neste sentido, todo e qualquer material que contenha Informações Confidenciais deverá ser mantido nas dependências da GESTORA, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa do superior hierárquico do Colaborador. Ainda, todo e qualquer arquivo eletrônico recebido ou gerado pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo do cliente ou do projeto a que se refere tal arquivo eletrônico.

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

Para fins de manutenção das Informações Confidenciais, a STRATEGI CAPITAL recomenda que seus Colaboradores:

(i) Bloqueiem o computador quando o mesmo não estiver sendo utilizado;
(ii) Mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro;
(iii) Descartem materiais usados, destruindo-os fisicamente;
(iv) Jamais revelem a senha de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem *Insider Trading*, Dicas ou *Front-running*, conforme definições adiante.

Insider Trading e "Dicas"

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

“Dica” é a transmissão, a qualquer terceiro, estranho às atividades da GESTORA, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

Front-running

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

O disposto nos itens acima deve ser analisado não só durante a vigência de seu relacionamento profissional com a GESTORA, mas também após o seu término.

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

Caso os Colaboradores tenham acesso, de forma indevida, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance, Risco e PLDFT, indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial indevida 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, acessarem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de Compliance, Risco e PLDFT 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 neste no manual de regras, procedimentos e controles internos da STRATEGI CAPITAL e na legislação aplicável, incluindo eventual demissão por justa causa.

2.2. Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela GESTORA para preservar o sigilo das Informações Confidenciais, na eventualidade de ocorrer o vazamento de quaisquer Informações Confidenciais, ainda que de forma

involuntária, o Diretor de Compliance, Risco e PLDFT deverá tomar ciência do fato tão logo seja possível.

De posse da Informação Confidencial, o Diretor de Compliance, Risco e PLDFT, primeiramente, identificará se a Informação Confidencial vazada se refere ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, o Diretor de Compliance, Risco e PLDFT procederá da seguinte forma:

(i) No caso de vazamento de Informações Confidenciais relativas aos fundos de investimento geridos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da Informação Confidencial atinente ao fundo de investimento.

(ii) No caso de vazamento de Informações Confidenciais relativas aos cotistas:

Neste caso, o Diretor de Compliance, Risco e PLDFT procederá com o tanto necessário para cessar a disseminação da Informação Confidencial ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (a) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (b) autorizar a contratação de advogados especializados na matéria; (c) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação Confidencial. Sem prejuízo, o Diretor de Compliance, Risco e PLDFT ficará à inteira disposição para auxiliar na solução da questão.

3. POLÍTICAS DE SEGREGAÇÃO DAS ATIVIDADES

3.1. Aspectos Gerais

Inicialmente, cumpre esclarecer que a STRATEGI CAPITAL atua exclusivamente como administradora de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros, não prestando, portanto, quaisquer outros serviços no mercado de capitais. Outrossim, visando atribuir o mais elevado grau de transparência, salienta-se que a STRATEGI CAPITAL possui somente a pessoa jurídica Strategi Capital Ltda. como sua controladora, cujo objetivo central da referida pessoa jurídica é a participação no capital da STRATEGI CAPITAL, não possuindo quaisquer outras empresas conglomeradas, coligadas, sob controle comum, controladoras ou controladas.

3.2. Ausência de conflitos de interesses

No tocante à sociedade Strategi Capital Ltda., conforme mencionado, o objetivo central da referida pessoa jurídica é a participação no capital da STRATEGI CAPITAL, não possuindo quaisquer outras empresas, conglomeradas, coligadas, sob controle comum, controladoras ou controladas. Em razão da inexistência de conflitos de interesses, a STRATEGI CAPITAL e a Strategi Capital Ltda. não adotam segregação física.

Sem prejuízo, cumpre salientar que para salvaguardar eventuais conflitos de interesse entre as áreas a GESTORA se utiliza das seguintes regras: (i) em primeiro lugar, existe a segregação lógica das áreas, sendo os acessos aos diretórios completamente segregados, com controle individual de acesso, de forma a garantir o máximo nível de confidencialidade das informações e manter o sigilo devido das operações realizadas pela GESTORA; (ii) todo e qualquer benefício recebido pela GESTORA diretamente ou indiretamente, serão integralmente revertidos aos seus clientes, conforme estabelecido na regulamentação em vigor. Ademais, eventuais rebates recebidos por investimentos feitos pelos fundos e/ou carteiras administradas geridos pela GESTORA serão devolvidos aos próprios fundos investidores e/ou às carteiras, exceto nos casos de investimentos feitos por (a) investidores profissionais que tenham assinado o Termo de Ciência previsto na Instrução CVM nº 555/2014, ou (b) fundo de investimento em cotas de fundo de investimento que invista mais de 95% (noventa e cinco por cento) de seu patrimônio em um único fundo de investimento.

Não obstante, a GESTORA atua exclusivamente como administradora de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros, não prestando, portanto, quaisquer outros serviços no mercado de capitais. Em razão disso, não é suscitada qualquer hipótese de conflito dentro da GESTORA. Não obstante, a STRATEGI CAPITAL manterá a devida segregação entre as suas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

O primeiro nível de segregação dentro das atividades da GESTORA refere-se às diferenças funcionais de atuação e autoridades definidas para as posições de gestor, analistas, compliance, risco e administrativo. Perfis de acesso, e o controle são realizados com base nessas divisões.

Apesar dessa segregação, para permitir que as atividades internas ocorram de modo eficiente, certas informações serão compartilhadas na base da necessidade (*as-needed basis*) nos comitês instituídos pela GESTORA, sendo que os participantes se responsabilizam pelo sigilo das informações.

O acesso de pessoas que não fazem parte do quadro de Colaboradores da STRATEGI CAPITAL será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio conhecimento e autorização da administração da STRATEGI CAPITAL, e desde que acompanhadas de Colaboradores da STRATEGI CAPITAL. Em caso de antigos Colaboradores, não será permitida a sua permanência nas dependências da STRATEGI CAPITAL, com exceção dos casos em que tenha sido chamado pela área de recursos humanos para conclusão do processo de desligamento, de aposentadoria ou outros. O atendimento a clientes nas dependências da STRATEGI CAPITAL deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

As diferentes áreas da GESTORA terão suas estruturas de armazenamento de informações logicamente segregada das demais, de modo a garantir que apenas os Colaboradores autorizados e necessários para o desempenho de determinada atividade tenham acesso às informações da mesma.

Sem prejuízo, as regras destacadas na política de segurança da informação, tratada neste documento, se aplicam para fins da presente política de segregação das atividades, e devem ser observadas pelos Colaboradores da GESTORA.

4. POLÍTICAS DE SEGURANÇA E SEGURANÇA CIBERNÉTICA

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da GESTORA e às disposições deste documento, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações da GESTORA são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

As estações de trabalho serão fixas, com computadores seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela GESTORA.

A coordenação direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo do Diretor de Compliance, Risco e PLDFT, que será o responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme aqui descrito.

4.1 Identificação de Riscos (*risk assessment*)

No âmbito de suas atividades, a GESTORA identificou os seguintes principais riscos internos e externos que precisam de proteção:

- Dados e Informações: as Informações Confidenciais;
- Sistemas: informações sobre os sistemas utilizados pela GESTORA e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;
- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da GESTORA; e
- Governança da Gestão de Risco: a eficácia da gestão de risco pela GESTORA quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a GESTORA identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais - ANBIMA:

- *Malware* – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);

- Engenharia social – métodos de manipulação para obter Informações Confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e *Acesso Pessoal*);

- Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da GESTORA;

- Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a GESTORA avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

4.2 Ações de Prevenção e Proteção

Após a identificação dos riscos, a GESTORA adota as medidas a seguir descritas para proteger suas informações e sistemas.

- Regra Geral de Conduta:

A GESTORA realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise.

Conforme mencionado na seção que trata da confidencialidade, é terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da GESTORA e circulem em ambientes externos à GESTORA com estes arquivos, uma vez que tais arquivos contêm Informações Confidenciais, observada a exceção mencionada na seção que trata da confidencialidade.

A troca de informações entre os Colaboradores da GESTORA deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida o Diretor de Compliance, Risco e PLDFT deve ser acionado previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da GESTORA qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Ademais, fica terminantemente proibido que os Colaboradores discutam ou acessem remotamente Informações Confidenciais, sendo que o acesso remoto de Informações Confidenciais é permitido em cenários de gestão de crise, conforme definido no plano de contingência e continuidade dos negócios.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter Informações Confidenciais mesmo no ambiente interno da GESTORA.

A GESTORA não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

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

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na GESTORA. É proibida a conexão de equipamentos na rede da GESTORA que não estejam previamente autorizados pela área de informática e pelos administradores da GESTORA.

O envio ou repasse por e-mail ou grupos de mensagens de celular que envolvam clientes ou parceiros comerciais 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 difamar a imagem e afetar a reputação da GESTORA.

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.

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

- Acesso Escalonado do Sistema

O acesso como “usuário” de área de *desktop* é limitado aos Colaboradores aprovados pelo Diretor de Compliance, Risco e PLDFT e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores. Adicionalmente, o acesso como “administrador” para manutenção das máquinas é exclusivo do Diretor de Compliance, Risco e PLDFT e do responsável pelo TI da GESTORA.

A GESTORA mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de *login* e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da GESTORA necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da GESTORA em caso de violação.

Todo Colaborador que tiver acesso aos sistemas de informação da GESTORA é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas.

É importante ressaltar que os acessos acima referidos são imediatamente cancelados em caso de desligamento do Colaborador da GESTORA.

- Senha e Login

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas semestralmente conforme aviso fornecido pelo responsável pelo TI da GESTORA.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

- Uso de Equipamentos e Sistemas

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

A utilização dos ativos e sistemas da GESTORA, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o Diretor de Compliance, Risco e PLDFT.

- Acesso Remoto

A GESTORA permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: a todos os Colaboradores, conforme requisição por estes e autorização pelo Diretor de Compliance, Risco e PLDFT, no que se refere ao acesso ao e-mail sendo que apenas os diretores da GESTORA e Colaboradores permitidos pela diretoria terão permissão de acesso à rede e ao diretório.

Ademais, os Colaboradores autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (iii) relatar ao Diretor de Compliance, Risco e PLDFT qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da GESTORA e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

- Controle de Acesso

O acesso de pessoas estranhas à GESTORA a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos administradores da GESTORA.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a GESTORA monitora a utilização de tais meios.

- *Firewall, Software*, Varreduras e Backup

A GESTORA utiliza um *hardware* de *firewall* projetado para evitar e detectar tentativas de conexões não autorizadas e incursões maliciosas. O Diretor de Compliance, Risco e PLDFT é responsável por determinar o uso apropriado de *firewalls* (por exemplo, perímetro da rede).

A GESTORA mantém proteção atualizada contra *malware* e tentativas de invasões nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, *vírus*, *worms*, *spyware*). Serão conduzidas varreduras semanais para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da GESTORA.

A GESTORA utiliza um plano de manutenção projetado para guardar os seus dispositivos e *softwares* contra vulnerabilidades com o uso de varreduras e patches. O

Diretor de Compliance, Risco e PLDFT é responsável por patches regulares nos sistemas da GESTORA.

A GESTORA mantém e testa regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance, Risco e PLDFT. As informações da GESTORA são atualmente objeto de backup diário com o uso de computação na nuvem.

4.3 Monitoramento e Testes

O Diretor de Compliance, Risco e PLDFT (ou pessoa por ele incumbida) adota as seguintes medidas para monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, semestral:

(i) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;
(ii) Monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela GESTORA para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da GESTORA; e
(iii) Verificação, por amostragem, das informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

O Diretor de Compliance, Risco e PLDFT poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

4.4 Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da GESTORA (incluindo qualquer violação efetiva ou potencial), deverá ser informada ao Diretor de Compliance, Risco e PLDFT prontamente. O Diretor de Compliance, Risco e PLDFT determinará quais membros da administração da GESTORA e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Compliance, Risco e PLDFT determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

- Procedimentos de Resposta

O Diretor de Compliance, Risco e PLDFT responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da GESTORA de acordo com os critérios abaixo:

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

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

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

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

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

(vi) Determinação do responsável (ou seja, a GESTORA ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance, Risco e PLDFT, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

4.5 Arquivamento de Informações

De acordo com o disposto neste documento, os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso IV do Artigo 16 da ICVM 558.

4.6 Propriedade Intelectual

Todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à GESTORA, tais como minutas de contrato, memorandos, cartas, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação bem como modelos de avaliação, análise e gestão, em qualquer formato, bem como todo e qualquer material produzido baseado em tais documentos e arquivos, são e permanecerão sendo propriedade exclusiva da GESTORA, 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 GESTORA, devendo todos os documentos permanecer em poder e sob a custódia da GESTORA, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da GESTORA, salvo se autorizado expressamente pela GESTORA e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize à GESTORA documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à GESTORA, o Colaborador deverá assinar declaração nos termos do Anexo IV ao manual de regras, procedimentos e controles internos da STRATEGI CAPITAL, confirmando 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 GESTORA, 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 GESTORA, exceto se aprovado expressamente pela GESTORA.

5. PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

5.1. Objetivo

Esse Plano de Contingência e Continuidade dos Negócios ("Plano de Contingência") tem como objetivo definir os procedimentos a serem adotados pela equipe da GESTORA, no caso de contingência, de modo a impedir descontinuidade operacional por problemas que impactem no funcionamento da GESTORA no âmbito da sua atividade de gestão de recursos. Foram estipulados estratégias e planos de ação com

o intuito de garantir que os serviços essenciais da GESTORA sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

Essas situações são classificadas de forma geral como contingências e implicam na modificação da rotina diária da operação, o que pode causar impactos financeiros, legais/regulatórios e de imagem, entre outros, à GESTORA.

5.2. Estrutura

Para atendimento às necessidades mínimas de manutenção dos serviços/atividades da GESTORA, foi definida uma estrutura mínima física, tecnológica e de pessoal, e procedimentos que devem ser adotados toda vez em que uma situação seja caracterizada como uma contingência às operações da GESTORA.

Foram identificados os seguintes focos de preocupação relativos à atividade de gestão de recursos que necessitam estar contemplados neste Plano de Contingência, de forma a garantir o regular funcionamento da GESTORA:

(i) Espaço Físico: local onde são realizadas as operações da GESTORA. Nesse espaço encontra-se instalada toda a infraestrutura necessária para a execução de suas atividades de gestão de recursos;

(ii) Tecnologia: fundamental para o funcionamento da GESTORA relativamente à gestão de recursos, no sentido de que todas as comunicações com clientes, corretoras, administradores de fundos etc., são realizados por telefone ou meios eletrônicos (e-mails e/ou sistemas próprios). Também é fundamental para a realização de registros de operações (compras e vendas de títulos, aplicações e resgates em fundos de investimento, transferência de recursos e pagamento de despesas da GESTORA, dentro outros); e

(iii) Pessoal: responsáveis pela operação da GESTORA, incluindo a análise e decisão para realização ou não de investimentos, equipe responsável pelo compliance e pela gestão de risco das carteiras etc.

Tendo identificado esses 3 (três) focos de preocupação do ponto de vista da estrutura da GESTORA e dos processos sob sua responsabilidade na qualidade de gestora de recursos, os riscos que podem ocasionar o acionamento do Plano de Contingência foram identificados da seguinte forma:

(i) Problemas de Infraestrutura: os problemas dessa ordem são, dentre outros, falta de energia elétrica, falha nos links de internet, falha nas linhas

telefônicas, falha ou inacessibilidade onde estão hospedados os sistemas utilizados pela GESTORA, falta de água etc.;

(ii) Problemas de acesso recursos: os problemas dessa ordem são, dentre outros, impossibilidade ou dificuldade de acesso aos recursos da GESTORA, especialmente planilhas e programas computacionais em virtude de problemas técnicos, inacessibilidade ou questões de cibersegurança; e

(iii) Falta impactante de Colaboradores: os problemas dessa ordem são, dentre outros, o término de vínculo repentino com pessoas chave para o funcionamento da GESTORA (notadamente seus diretores), o não comparecimento de número expressivo de Colaboradores em razão de doenças ou qualquer outro tipo de impedimento etc.

Com base no levantamento da estrutura da GESTORA relativa à gestão de recursos e no mapeamento de riscos, a GESTORA tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações e/ou no caso de falta impactante de Colaboradores ao local de trabalho. Adicionalmente, a GESTORA investe recursos significativos em equipamentos, softwares e outros recursos computacionais para reforçar a segurança e proteção em torno dos seus ativos computacionais.

Conforme avaliação de risco da GESTORA foram definidas as seguintes ações a serem tomadas quando da ativação do Plano de Contingência:

- Ambiente Físico

O ambiente físico é definido como o espaço onde as operações diárias de gestão de recursos da GESTORA são conduzidas normalmente. Esse espaço inclui o imóvel, os móveis e utensílios necessários a essa operação, como também o acesso seguro a esses recursos.

Em ocorrendo situações de problemas de acesso às suas dependências, a equipe da GESTORA deve continuar a desempenhar suas atividades através de *home office*, uma vez que todos os arquivos podem ser acessados pela nuvem. Além disso, há a vinculação dos e-mails e seu armazenamento pela suíte de aplicativos Office 365 da Microsoft. Assim, é possível permanecer trabalhando ainda que fora do escritório da GESTORA.

- Ambiente Tecnológico

O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a GESTORA possa realizar sua operação de forma normal. Isso implica basicamente a disponibilidade de acesso aos sistemas utilizados pela GESTORA para a gestão de recursos em seu dia a dia e garantia de que suas informações estejam protegidas e possam ser acessadas e/ou utilizadas na operação da GESTORA, que inclui o armazenamento de dados de sistemas e aplicativos, os equipamentos eletrônicos em geral, links de telecomunicação e transmissão de dados, softwares e computadores, aparelhos telefônicos etc., incluindo os recursos necessários para que tais itens funcionem de forma adequada e segura.

A GESTORA conta com práticas de alta disponibilidade em sua infraestrutura de tecnologia de informação. A infraestrutura física de tecnologia da GESTORA é coberta por nobreaks para garantir a continuidade das operações em caso de queda da energia elétrica. Contando também com redundância automática de links de internet para incrementar a disponibilidade nesta.

Todos os sistemas utilizados pela GESTORA são acessados através de sites dos próprios provedores desses sistemas, o que viabiliza acessá-los de qualquer local desde que se disponha de um computador com um link de internet, permitindo, portanto, fácil acesso remoto.

Diariamente são realizados backups dos dados armazenados na “nuvem” em servidores internos, possibilitando acesso aos dados em caso de indisponibilidade de comunicação com o sistema. A Gestora dispõe de firewalls para proteger toda a infraestrutura dentro da rede local e, de forma a manter seu time alerta com questões relacionadas à cibersegurança, conforme detalhado neste documento.

A comunicação com clientes, corretoras, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares da equipe da GESTORA. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência da GESTORA, de forma a que estes também tenham conhecimento da situação tão logo ela ocorra, buscando impactar o mínimo possível a operação de gestão de recursos da GESTORA.

- Ambiente Pessoal

O ambiente pessoal envolve todos os Colaboradores e prestadores de serviços existentes na GESTORA relacionados à atividade de gestão de recursos. Suas funções devem atender às necessidades de funcionamento da GESTORA em situações consideradas de normalidade bem como em situações consideradas de contingência.

Este Plano de Contingência visa atribuir prioridades e responsabilidades à equipe da GESTORA de forma a impactar o mínimo possível em suas atividades em situação de contingência.

O principal ponto de risco seria a não existência de um backup de atividades executadas por um determinado Colaborador. Esse risco, no entanto, não é considerado como relevante pois o sistema contratado junto à Microsoft realiza backups instantâneos, automáticos e persistentes de arquivos, planilhas e demais documentos salvos nas pastas de trabalho de cada Colaborador. Devido aos backups persistente, mesmo em caso de saída temporária por qualquer razão, desligamento ou mesmo ato de má fé praticado por determinado(s) Colaborador(es), a GESTORA continuará tendo acesso aos arquivos.

5.3. Equipe de Contingência

Para coordenar todas as ações necessárias em situações de contingência bem como promover o adequado treinamento e ações para restabelecimento da situação de atividade normal da GESTORA, foram definidos os seguintes responsáveis pela Equipe de Contingência:

- Diretor de Compliance, Risco e PLDFT (Coordenador de Contingência);
- Responsável pelo TI; e
- Analista de Compliance, risco e PLDFT.

Essas pessoas deverão tomar as decisões necessárias para acionar este Plano de Contingência se e quando necessário, tomando essa decisão em conjunto ou, no caso de impossibilidade, com os demais administradores da GESTORA.

5.4. Cenários de Contingência

Neste cenário, considera-se basicamente a impossibilidade ou dificuldade em manter o funcionamento normal da GESTORA devido a problemas de ordem técnica (hardware), física (acesso ao escritório), pessoal (ausência significativa de colaboradores) e de infraestrutura (falta de energia).

Nessa situação, o Coordenador de Contingência deverá acionar este Plano de Contingência, em caráter imediato, e iniciar também imediatamente a avaliação das causas que geraram a contingência para providenciar sua solução o mais rapidamente possível, bem como dar início ao efetivo cumprimento dos procedimentos descritos abaixo, quais sejam:

(i) Comunicar imediatamente o ocorrido à toda a equipe interna, via ligação celular, grupo corporativo da empresa em aplicativo de mensagens ou qualquer outro meio à sua disposição, indicando nessa oportunidade qual o procedimento a ser adotado por cada Colaborador de acordo com a contingência ocorrida;

(ii) (b) Caso seja verificada a necessidade de sair do escritório da GESTORA, os Colaboradores poderão continuar a desempenhar suas atividades através de *home office*. A continuidade das operações da GESTORA deverá ser assegurada no próprio dia útil da ocorrência da contingência no escritório físico, de modo que as atividades diárias não sejam interrompidas ou gravemente impactadas.

O Coordenador de Contingência deverá acompanhar todo o processo acima descrito até o retorno à situação normal de funcionamento dentro do contexto das atividades desempenhadas pela GESTORA e reportar eventuais alterações e atualizações da contingência aos demais colaboradores.

5.5. Aspectos Gerais

É responsabilidade do Coordenador de Contingência manter este Plano de Contingência atualizado, bem como a realização de validação anual dos procedimentos estabelecidos neste Plano de Contingência.

Ainda, o Coordenador de Contingência realizará testes de contingências que possibilitem que a GESTORA esteja preparada para eventos desta natureza, proporcionando à GESTORA condições adequadas para continuar suas operações.

Sendo assim, anualmente, é realizado um teste de contingência para verificar:

(i) Acesso aos sistemas;
(ii) Acesso ao e-mail corporativo;
(iii) Acesso aos dados armazenados;
(iv) Verificação do treinamento aos Colaboradores para atuarem como backup; e
(v) Qualquer outra atividade necessária para continuidade do negócio.

O resultado do teste é registrado em relatório, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano de Contingência.

6. TREINAMENTO

O Diretor de Compliance, Risco e PLDFT organizará treinamento anual dos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de Compliance, previsto no manual de regras, procedimentos e controles internos da STRATEGI CAPITAL.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta política de segregação, confidencialidade, segurança da informação e segurança cibernética será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

Histórico das atualizações		
Data	**Versão**	**Responsáveis**
Agosto de 2020	1ª e Atual	Diretor de Compliance, Risco e PLDFT