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

R CAPITAL ASSET MANAGEMENT INVESTIMENTOS S.A.

JANEIRO/2024

V. 3.0.

I. OBJETO

A presente Política de Confidencialidade, Segregação, Segurança da Informação e Segurança Cibernética da **R CAPITAL ASSET MANAGEMENT INVESTIMENTOS S.A.** (“R Cap” ou “Gestora”) tem por objetivo, de forma geral, descrever as regras adotadas pela Gestora para garantir a segurança das suas informações mais sensíveis, bem como abordar os procedimentos definidos para segurança cibernética.

Esta política se aplica aos sócios, administradores, funcionários e todos que, de alguma forma, auxiliam o desenvolvimento das atividades da Gestora.

SUMÁRIO

1. Confidencialidade

Todas as informações que se referem a sistemas, negócios, estratégias, posições ou a clientes da Gestora são confidenciais e devem ser tratadas como tal, sendo utilizadas apenas para desempenhar as atribuições na Gestora e sempre em benefício dos interesses desta e de seus clientes.

Toda e qualquer informação que os Colaboradores tiverem com relação aos clientes da Gestora deve ser mantida na mais estrita confidencialidade, não podendo ser divulgada sem o prévio e expresso consentimento do cliente, salvo na hipótese de decisão judicial específica que determine à Gestora a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório da Comissão de Valores Mobiliários ("CVM"). Caso a Gestora ou qualquer dos Colaboradores sejam obrigados a revelar as informações de clientes em face de procedimento judicial ou extrajudicial da CVM, tal fato deve ser seguido de imediata e expressa comunicação aos clientes afetados, caso não haja norma dispondo de forma diversa.

Os Colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto à Gestora, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pela Gestora. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à administração da Gestora, para que sejam tomadas as medidas cabíveis.

A Gestora exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Gestora, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

Todo e qualquer material com informações de clientes ou de suas operações 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 (rede corporativa - nuvem) exclusivo do cliente ou do projeto a que se refere tal arquivo eletrônico.

Para fins de manutenção das informações confidenciais, a Gestora 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 e (iv) jamais revelem a senha de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

2. Segurança da Infomação

2.1. Aspectos Gerais

No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, sejam dos clientes ou das operações a eles relacionadas, ficam armazenadas em serviços de armazenamento de dados na nuvem (cloud computing), cujo acesso é permitido apenas aos colaboradores da Gestora, conforme atribuições, além dos administrados pelos membros do departamento de informática.

Todo software disponibilizado aos Colaboradores deverá ser utilizado somente para os negócios da Gestora, em consonância com os acordos de licenciamento firmados.

A realização de back up de todas as informações ocorre em servidores de nuvem (One Drive), com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

O acesso aos sistemas de informação da Gestora é feito por meio de um par "usuário/senha" que permite ao responsável pelo departamento de informática acompanhar, de forma precisa, as atividades desenvolvidas por cada um dos Colaboradores. O acesso e o uso de qualquer informação, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da Gestora. O controle desses dados é de domínio da Gestora, uma vez que o armazenamento dos dados ocorre em servidores de nuvem (One Drive), garantindo, assim, a confidencialidade e confiabilidade da informação.

Para acessar informações nos sistemas da Gestora deverão ser utilizadas somente ferramentas e tecnologias autorizadas e previamente estabelecidas pela Gestora, de forma a permitir a identificação e rastreamento de quais usuários tiveram acesso a determinadas informações (os logs de acesso ficam armazenados nos sistemas).

Adicionalmente, informamos que a rede da Gestora é composta por diretórios de dois níveis: (i) diretórios de informações públicas, aos quais todos os Colaboradores têm acesso, contendo tão somente informações de natureza administrativa; e (ii) diretórios de acesso restrito, cujo acesso é somente pré-autorizado pelo Diretor de Compliance, Risco e PLD aos membros de alguns departamentos específicos.

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. O Colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não os divulgar a terceiros em qualquer hipótese.

Colaboradores, quando de sua contratação, devem assinar o Termo de Confidencialidade da Gestora, presente na Política de Regras, Procedimentos e Descrição dos Controles Internos, Elaborados para o Cumprimento da Resolução 21/21, pelo qual se obrigam, entre outras coisas, a proteger a confidencialidade das informações a que tiverem acesso enquanto estiverem trabalhando na Gestora e durante certo período após terem deixado a Gestora.

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

A Gestora se reserva o direito de proibir o uso de telefones celulares na área de gestão e de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via internet, ou mesmo intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, como os arquivos armazenados ou criados pelos recursos da informática pertencentes à Gestora ou utilizados em nome dela, a fim de assegurar o fiel cumprimento desta política de Segurança da Informação, bem como da legislação em vigor.

2.2. Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais, Reservadas ou Privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Gestora (“Informações” ou “Informação”), na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de Compliance, Risco e PLD deverá tomar ciência do fato tão logo seja possível.

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

I. No caso de vazamento de Informações 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. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

II. No caso de vazamento de Informações relativas aos cotistas:

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

2.3. Testes Periódicos

Periodicamente, a Gestora realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

(i) Anualmente, altera-se a senha de acesso dos Colaboradores;
(ii) Testes no firewall;
(iii) Testes nas restrições impostas aos diretórios;
(iv) Manutenção trimestral de todo o "hardware" por empresa especializada em consultoria de tecnologia de informação;
(v) Testes no "back-up" (salvamento de informações), realizado em nossa nuvem.

3. Segregação de Atividades

Inicialmente, cumpre esclarecer que 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. Não obstante, a Gestora manterá a devida segregação entre as suas diversas 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.

A atividade de administração de carteira de valores mobiliários é exaustivamente regulada pela CVM, com a exigência de credenciamento específico e está condicionada a uma série de providências, dentre elas a segregação total de suas atividades de administração de carteiras de valores mobiliários de outras que futuramente possam vir a ser desenvolvidas pela Gestora ou empresas controladoras, controladas, ligadas ou coligadas, bem como prestadores de serviços.

A segregação 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 de Compliance, Risco e Administrativo, sendo que os participantes se responsabilizam pelo sigilo das informações.

O acesso de pessoas que não fazem parte do quadro de Colaboradores da Gestora será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio conhecimento e autorização da administração da Gestora, e desde que acompanhadas de Colaboradores da Gestora. Em caso de antigos Colaboradores, não será permitida a sua permanência nas dependências da Gestora 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 Gestora 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, sobretudo no que tange às segregações eletrônicas e de funções, se aplicam para fins da presente política de Segregação das Atividades, e devem ser observadas pelos Colaboradores.

4. Procedimento de Segurança Cibernética

Responsável: o Diretor de Compliance, Risco e PLD da Gestora.

4.1. Identificação e Avaliação

A Gestora deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de cybercriminals são os seguintes:

a. Malware (vírus, cavalo de troia, spyware e ransomware);
b. Engenharia Social;
c. Pharming;
d. Phishing scam;
e. Vishing;
f. Smishing;
g. Acesso pessoal;
h. Ataques de DDoS e botnets;
i. Invasões (advanced persistent threats).

Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, a Gestora definiu todos os ativos relevantes da instituição, fundamentais a seu funcionamento, criou regras para classificação das informações geradas e avalia continuamente a vulnerabilidade de cada um desses ativos.

A Gestora levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

Utilizamos softwares de alta reputação, que são escolhidos pelo alto grau de segurança o qual nos certifica a uma baixa vulnerabilidade dos riscos cibernéticos.

4.2. Ações de Prevenção e Proteção

Uma importante regra de prevenção consiste na segregação de acessos a sistemas e dados que a Gestora adota, conforme já detalhado nas regras internas que tratam de Compliance e Segurança da Informação.

A Gestora adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. A Gestora trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis. A Gestora deve criar logs e trilhas de auditoria sempre que os sistemas permitam.

O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados, a critério do responsável pela Segurança Cibernética.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a Gestora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção. A Gestora conta com recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais. A Gestora deve, adicionalmente, proibir o acesso a determinados websites e a execução de softwares e/ou aplicações não autorizadas.

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 que são consideradas como Informações Confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pelo Diretor de Compliance, Risco e PLD.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a 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.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais, devendo, portanto, evitar o uso indiscriminado deles para fins pessoais.

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 Gestora, bem como avisar prontamente o Diretor de Compliance, Risco e PLD.

Não obstante o disposto no parágrafo anterior, todos os anexos dos e-mails recebidos pelos Colaboradores da Gestora são rigidamente verificados pelos servidores, de modo que os Colaboradores sequer receberão e-mails que tenham sido identificados como suspeitos após tal verificação.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente, bem como são criptografadas com chaves de 128 bits, dificultando, portanto, sua decodificação e, consequentemente, a utilização dos logins dos Colaboradores por terceiros não autorizados.

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

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 Gestora adota também backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do plano de continuidade dos negócios da Gestora.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas 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 Resolução 21/21, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

Para concluir, pode-se mencionar que as medidas de diligência prévia também são relevantes à prevenção e proteção dos ativos da Gestora e devem ser observadas integralmente.

4.3. Mecanismos de Supervisão para cada Risco Identificado

Utilizamos Firewalls, Antivírus além de termos como prática a troca constante de senhas pessoais.

4.4. Testes Realizados

O Diretor de Compliance, Risco e PLD deve se assegurar de que os mecanismos de controle descritos acima, dentre outros são anualmente testados pela equipe responsável.

A gestora possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. A Gestora mantém inventários

atualizados de hardware e software, e verifica-os com frequência para identificar elementos estranhos à instituição.

A área responsável da Gestora deve diligenciar para manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

A área responsável deve também monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados.

Deve-se, ademais, realizar testes de invasão externa, phishing, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

Os logs e trilhas de auditoria criados na forma definida no item anterior devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

Por fim, o Diretor de Compliance, Risco e PLD deverá verificar, aleatoriamente, (i) os e-mails repassados pelos Colaboradores, (ii) o modo adotado pelos Colaboradores para utilização dos ativos, sistemas, servidores e rede de informações da Gestora, incluindo a verificação de sites visitados, e (iii) do histórico de acessos às áreas restritas da Gestora.

4.5. Plano de Resposta

A Área de Gestão de Riscos e de Compliance deve, conjuntamente com os profissionais de cybersecurity e Segurança da Informação, elaborar um plano formal de resposta a ataques virtuais. A Gestora deverá estabelecer os papeis de cada área em tal plano, prevendo o acionamento de Colaboradores-chave e contatos externos relevantes.

O plano de resposta deverá levar em conta os cenários de ameaças previstos no risk assessment. Deve haver critérios para a classificação dos incidentes, por severidade. O plano deve prever, conforme o caso, o processo de retorno às instalações originais após o final do incidente, na hipótese em que as instalações de contingência ou acessos remotos tenham de ser utilizados.

4.6. Reciclagem e Revisão

O programa de segurança cibernética, que contempla os procedimentos aqui descritos, o plano formal de resposta e demais políticas internas da Gestora sobre a matéria, deverá ser revisto e atualizado anualmente.

Os grupos de trabalho diretamente envolvidos com qualquer parte do programa devem se manter atualizados, buscando fornecedores especializados, se necessário.

A Gestora deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

Os Colaboradores deverão participar de treinamentos que abordem o tema da segurança cibernética, os quais serão aplicados pelo responsável pela presente política, em periodicidade não superior a 12 (doze) meses.

4.7. Vigência e Atualização

A presente Política 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**	**Responsável**
Março de 2021	1.0	Diretor de Compliance, Risco e PLD/FTP
Janeiro de 2023	2.0	Diretor de Compliance, Risco e PLD/FTP
Janeiro de 2024	3.0	Diretor de Compliance, Risco e PLD/FTP

Anexo 1

PCN | Processos Críticos

Processo	Área	Atividade	Recursos	Plano de Continuidade Operacional
Negociação de ativos	GF	Emissão de boleta	• Teams: aplicação/resgate de cotas • E-mail: compra e venda de ativo	• HO: Celular ou computador pessoal
Negociação de ativos	Back	Boletagem de ativos (Administrador)	• Vortx: boletador (site Vortx) ou e-mail • Terra: via e-mail	• HO: Celular ou computador pessoal (necessita de login e senha da Vortx)
Gestão de caixa	GF	Apuração/divulgação/disponibilização de provento a ser pago por cota - dividendos	• One drive	• HO: Celular ou computador pessoal
Gestão de caixa	GF	Disponibilizar recurso para investidas	• APP Banco	• HO: Celular ou computador pessoal (necessita de login e senha do Banco)
Operacional - investidas	Back	Envio de dinheiro para conta da Land (Fundo x Land)	• APP Banco Bradesco; Conta Vortx; Conta Terra	• HO: Celular ou computador pessoal (necessita de login e senha do Banco)
Operacional - investidas	Back	Envio de dinheiro para conta da SPE (Land x SPE)	• APP Banco Itaú	• HO: Celular ou computador pessoal (necessita de login e senha do Banco)
Operacional - investidas	Back	Pagamentos Land (contabilidade, advogado)	• APP Banco Itaú	• HO: Celular ou computador pessoal (necessita de login e senha do Banco)

Riscos potenciais

- Ausência de informações necessárias para apuração de dividendos (maior risco no fechamento do semestre)
- Ausência de recurso disponível na conta do Fundo para pagamento de obrigações:
  - Dividendos
  - Pagamentos Land, envio de dinheiro para Land/SPE

Figura 1 - Processos e atividades considerados como críticos, planos de contingência, responsáveis e riscos potenciais