POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

GENESIS CAPITAL GESTORA DE RECURSOS LTDA.

Agosto de 2026 – Versão 4.0

ÍNDICE

I. OBJETIVO

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") tem por objetivo estabelecer regras, procedimentos e controles internos para assegurar Confidencialidade, Disponibilidade, Integridade e Autenticidade aos Ativos de Informação da Genesis Capital Gestora de Recursos Ltda. ("Genesis Capital" ou "Gestora").

II. APLICABILIDADE

Esta Política aplica-se a todas as pessoas físicas e jurídicas que atuem, direta ou indiretamente, em nome da Genesis Capital ou em seu benefício, independentemente da natureza do vínculo mantido. Todos os seus destinatários deverão conhecer, compreender e observar as disposições desta Política, adotando conduta compatível com as diretrizes de segurança da informação, segurança cibernética, privacidade e proteção de dados, sem prejuízo do cumprimento das demais obrigações legais, regulatórias e internas aplicáveis.

Para assegurar sua efetiva implementação, divulgação e observância, a Gestora deverá promover a ampla disseminação desta Política a todos os públicos a ela sujeitos, garantindo sua disponibilização no *website* da Genesis. Adicionalmente, deverá manter evidências da ciência, adesão e capacitação dos seus colaboradores, conforme aplicável (vide Anexo I).

A Gestora pode solicitar a terceiros comprovações de conformidade com requisitos de segurança da informação, segurança cibernética e proteção de dados, sempre que o risco da relação ou exigências regulatórias justificarem. Essa comprovação pode ocorrer por meio de políticas, procedimentos, controles internos, questionários de *due diligence,* evidências de treinamentos, relatórios de conformidade e outros documentos necessários para a avaliação adequada dos riscos.

III. APROVAÇÃO, VIGÊNCIA E ATUALIZAÇÃO

Esta versão entra em vigor na data de sua publicação e será revisada em prazo não superior a 24 (vinte e quatro) meses, ou sempre que ocorrer: (i) alteração legal, regulatória ou de autorregulação relevante; (ii) incidente relevante de segurança; (iii) mudança significativa de tecnologia, processos ou sistemas; ou (iv) alteração material nos riscos identificados.

IV. ARCABOUÇO NORMATIVO

Este instrumento foi elaborado para atender ao previsto nas seguintes normas e diretrizes: (i) Resolução CVM nº 21 ("RCVM 21"); (ii) Guia de Cibersegurança (Anbima);

(iii) Orientações para Contratação de terceiros e Nuvem (Anbima); (iv) Orientações para Compartilhamento de Informações de Incidentes Cibernéticos(Anbima); (v) Orientações para o treinamento de colaboradores em Cibersegurança (Anbima); (vi) Orientações na Gestão de Continuidade de Negócios (Anbima); (vii) Orientações para a Implementação de Políticas de BYOD (Anbima); (viii) Lei nº 13.709/2018 ("LGPD"); e (ix) normas da Agência Nacional de Proteção de Dados ("ANPD").

V. GOVERNANÇA

O Compliance é responsável pela administração, supervisão e acompanhamento do cumprimento desta Política, incluindo a definição de controles, a avaliação periódica de sua efetividade, o tratamento de não conformidades e a proposição de medidas corretivas e de aprimoramento.

Para fins de suporte técnico à implementação, operação e monitoramento dos controles de segurança da informação e segurança cibernética, a Gestora poderá contar com prestadores de serviços especializados, cuja atuação ocorrerá sob supervisão do Compliance e em conformidade com os requisitos estabelecidos nesta Política.

O monitoramento dos controles de segurança da informação e segurança cibernética deverá ocorrer de forma contínua e compatível com a natureza, porte, complexidade e perfil de risco das atividades desenvolvidas pela Gestora.

VI. DEFINIÇÕES

Para fins desta Política, considera-se:

a) SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
b) SEGURANÇA CIBERNÉTICA: ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;
c) SEGURANÇA DE DADOS PESSOAIS: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais[1] de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

[1] **dado pessoal:** informação relacionada a pessoa natural identificada ou identificável; **dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; **dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

d) RISCO: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

e) RISCO DE SEGURANÇA DA INFORMAÇÃO: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

f) RISCO CIBERNÉTICO: perda de confidencialidade, integridade, controle ou disponibilidade de informações ou tecnologias com possíveis impactos adversos a operações, atividades, funções, ativos, indivíduos, organizações ou nações.

g) INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

h) INCIDENTE DE SEGURANÇA DE DADOS PESSOAIS: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais (Resolução CD/ANPD Nº 15, de 24 de abril de 2024);

i) INCIDENTE CIBERNÉTICO[2]: Incidente cibernético é qualquer evento ou tentativa que possa comprometer a disponibilidade, integridade, confidencialidade ou autenticidade de sistemas e informações. Inclui acessos não autorizados, exploração de vulnerabilidades, alterações indevidas em sistemas, ataques de negação de serviço (DoS/DDoS) e outras ações que afetem dados ou operações. A ocorrência de um incidente não significa necessariamente que houve comprometimento das informações, mas que elas estão sob ameaça. Exemplos incluem malware, phishing e outras técnicas de engenharia social, invasões, ataques de força bruta e interceptação de comunicações; e

j) BRING YOUR OWN DEVICE (BYOD): permite que os dispositivos pessoais dos funcionários sejam usados nas atividades corporativas. Uma política BYOD estabelece limitações e restrições sobre se um dispositivo pessoal (como um notebook, smartphone ou tablet) pode ou não ser conectado pela rede corporativa.

VII. PRINCÍPIOS E DIRETRIZES ADOTADOS

a) Clássicos da Segurança da Informação (“CIDA”):

[2] Exemplos não exaustivos: **Malware** (e.g. ransomware, vírus, worms, trojans, spyware, adware, rootkits, screenlogger, bots) – softwares desenvolvidos para corromper computadores e redes; **Engenharia social** (e.g. clickjacking; phishing, quishing, smishing, vishing, deepfake) – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito; **Ataques de DoS** (Negação de Serviços), DDoS (Negação de Serviço Distribuída) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da organização, no caso das botnets, o ataque vem de muitos computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços; **Intrusões** (e.g. ataque de força bruta e MitM – Man in the Middle, em que um invasor se insere entre duas partes que estão se comunicando, interceptando e, potencialmente, modificando a comunicação sem que nenhuma das partes saiba) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

(i) **Confidencialidade:** propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

(ii) **Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas (acidentais ou propositais), durante todo o seu ciclo de vida (em repouso ou durante sua transmissão);

(iii) **Disponibilidade:** garantir que as informações estejam disponíveis sob demanda, conforme acordo prévio, a todas as pessoas autorizadas; e

(iv) **Autenticidade**: garantir que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

b) **Diretrizes Complementares:**

(i) **Segregação de Funções:** distribuição de responsabilidades para reduzir riscos de fraude, erro ou abuso de privilégios.

(ii) **Abordagem Baseada em Riscos (ABR):** implementar controles de segurança proporcionais à criticidade dos ativos, às ameaças identificadas e aos impactos potenciais para a Gestora, seus clientes e demais partes interessadas.

(iii) **Resiliência Cibernética:** assegurar a capacidade de prevenir, resistir, responder, recuperar-se e adaptar-se a incidentes cibernéticos, preservando a continuidade das atividades e a integridade dos serviços prestados.

c) **Básicos de Privacidade e Proteção de Dados:**

(i) **Privacidade e Proteção de Dados:** garantir que o tratamento de dados pessoais seja realizado com boa-fé e em conformidade com a Lei nº 13.709/2018.

(ii) **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

(iii) **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

(iv) **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

(v) **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

(vi) **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

(vii) **Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

(viii) **Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

(ix) **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

(x) **Não Discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

(xi) **Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

VIII. ATIVOS DE INFORMAÇÃO

Para fins desta Política, considera-se:

a) ATIVO: qualquer recurso tangível ou intangível que possua valor para a Gestora e que contribua para o desempenho de suas atividades, incluindo informações, pessoas, processos, sistemas, aplicações, equipamentos, infraestrutura, serviços e instalações;

b) ATIVOS DE INFORMAÇÃO: dados e informações de qualquer natureza e todos os recursos utilizados para sua criação, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, proteção ou descarte, incluindo documentos físicos e eletrônicos, bases de dados, sistemas, aplicações, equipamentos, dispositivos, serviços de tecnologia, infraestrutura, ambientes físicos, recursos em nuvem, processos e pessoas que tenham acesso ou responsabilidade sobre tais informações.

A Gestora manterá atualizado o controle de seus ativos de informação e recursos tecnológicos, bem como realizará a identificação e o acompanhamento de vulnerabilidades por meio de testes e monitoramentos periódicos de TI.

IX. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações devem ser classificadas de acordo com a sua natureza, sensibilidade, criticidade e necessidade de proteção, de modo a assegurar a adoção de controles adequados para o tratamento durante todo o seu ciclo de vida.

As informações classificadas como mais sensíveis ou críticas estarão sujeitas a medidas adicionais de segurança.

Para os fins desta Política, a classificação das informações deverá observar as seguintes categorias:

(i) **Pública**: informação cuja divulgação é autorizada ou exigida por disposição legal, regulatória ou contratual, destinada ao público em geral ou a partes externas, sem restrições de acesso e cujo compartilhamento não acarreta riscos à Gestora, aos seus clientes ou a terceiros.

(ii) **Interna:** informação destinada ao uso interno da Gestora, cujo acesso é permitido aos colaboradores e terceiros autorizados. Sua divulgação não autorizada pode causar impactos limitados de natureza operacional, administrativa ou reputacional.

(iii) **Confidencial:** informação cujo acesso deve ser restrito a pessoas autorizadas, em razão de sua relevância para as atividades da Gestora, de seus clientes ou de terceiros. Sua divulgação, alteração ou utilização não autorizada pode causar impactos financeiros, operacionais, regulatórios, reputacionais ou legais à Gestora, aos seus clientes ou a terceiros.

(iv) **Privilegiada**[3]**:** informação relevante ainda não divulgada ao mercado ou ao público em geral, obtida em decorrência de relacionamento profissional ou pessoal com clientes, emissores, sociedades investidas, contrapartes ou terceiros. O acesso a informações privilegiadas deve observar as disposições legais e regulatórias aplicáveis, devendo tais informações ser mantidas em sigilo por todos aqueles que delas tenham conhecimento.

(v) **Restrita:** informação submetida ao mais elevado nível de controle de acesso, disponibilizada exclusivamente a pessoas, funções ou áreas especificamente autorizadas. Sua divulgação, alteração ou utilização não autorizada pode causar danos à estratégia, às operações, à segurança, à conformidade regulatória ou aos interesses da Gestora e de seus clientes.

[3] Vide Lei nº 6.385, de 7 de dezembro de 1976.

Informações classificadas como Internas, Confidenciais, Privilegiadas ou Restritas não poderão ser compartilhadas ou discutidas em locais públicos, ambientes não seguros ou com pessoas não autorizadas.

As informações da Genesis Capital, de seus clientes, fundos e operações somente poderão ser divulgadas a terceiros, inclusive órgãos reguladores, autoridades, imprensa ou demais partes externas, por pessoas devidamente autorizadas pela Diretoria de Compliance ou em cumprimento de obrigação legal, regulatória ou contratual aplicável.

Todos os profissionais e terceiros vinculados à Gestora deverão preservar a confidencialidade das informações às quais tiverem acesso, evitando sua divulgação, utilização ou compartilhamento indevido.

O uso de ferramentas de inteligência artificial para fins corporativos dependerá de avaliação prévia do Diretor de Compliance quanto aos requisitos de segurança, privacidade e proteção de dados. É proibida a inserção de informações confidenciais, privilegiadas ou restritas em ferramentas públicas de IA sem autorização prévia e sem a devida validação dos riscos envolvidos.

A gestão das informações deve ser realizada por meio de um processo de melhoria contínua, governança e monitoramento, observando, no mínimo, os seguintes mecanismos:

(i) Classificação de informações: as informações são classificadas de acordo com sua natureza, sensibilidade e criticidade, sendo os controles de acesso, armazenamento, compartilhamento, transmissão e descarte definidos de forma proporcional ao respectivo nível de classificação;

(ii) Mesa e Tela Limpas: A Genesis Capital adota práticas de Mesa Limpa e Tela Limpa, de forma que documentos físicos, mídias, anotações, dispositivos e demais informações classificadas não permaneçam expostos quando não estiverem em uso. Os colaboradores deverão armazenar adequadamente documentos e equipamentos ao se ausentarem de suas estações de trabalho, bem como bloquear suas telas sempre que deixarem seus equipamentos sem supervisão;

(iii) Equipamentos e Estrutura: Os equipamentos, sistemas, aplicações e demais ativos tecnológicos da Gestora deverão ser mantidos atualizados e protegidos por medidas de segurança adequadas, incluindo controles de acesso, proteção contra ameaças e realização periódica de backups testados.

(iv) Armazenamento de Dados e Computação em Nuvem: Os serviços de armazenamento de dados e computação em nuvem utilizados pela Gestora deverão ser submetidos a processo de avaliação e monitoramento periódico, considerando requisitos de segurança da informação, segurança cibernética,

proteção de dados, continuidade dos negócios e capacidade técnica dos fornecedores.

(v) **Gerenciamento de Acesso:** O acesso às informações e aos sistema será limitado às necessidades de cada usuário, mediante controles de autenticação, monitoramento e revisão periódica, observadas as exigências da LGPD.

(vi) **Capacitação e Treinamento**: Todos os colaboradores e terceiros relevantes deverão participar de treinamentos periódicos sobre Segurança da Informação, Segurança Cibernética, Privacidade e Proteção de Dados, cuja efetividade poderá ser avaliada por meio de testes e ações de conscientização.

X. PROGRAMAS DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

A Genesis Capital manterá Programa de Segurança da Informação e Segurança Cibernética compatível com a natureza, porte, complexidade e perfil de risco de suas atividades, destinado à identificação, avaliação, tratamento, monitoramento e resposta aos riscos capazes de afetar a confidencialidade, integridade, disponibilidade e autenticidade dos seus Ativos de Informação.

O Programa deverá considerar ameaças internas e externas, incluindo falhas humanas, vulnerabilidades tecnológicas, indisponibilidade de sistemas, engenharia social, códigos maliciosos, acessos não autorizados, comprometimento de credenciais, falhas de terceiros, falhas operacionais e quaisquer outros eventos que possam comprometer a segurança das informações, dos sistemas ou da continuidade das atividades da Gestora.

Para a adequada gestão desses riscos, a Genesis Capital deverá identificar e avaliar periodicamente seus processos, ativos de informação, sistemas, equipamentos, dados, recursos tecnológicos e prestadores de serviços relevantes, de modo a determinar os controles de prevenção, proteção, detecção, resposta e recuperação compatíveis com os riscos identificados.

XI. GESTÃO DE RISCOS

A avaliação dos riscos de segurança da informação e segurança cibernética será coordenada pelo Compliance, com apoio dos prestadores de serviços e profissionais envolvidos, quando necessário.

A Gestora realizará avaliação dos riscos relacionados aos seus sistemas, informações, processos e prestadores de serviços relevantes, bem como reavaliações sempre que houver alterações relevantes em suas operações, tecnologias utilizadas ou após a ocorrência de incidentes significativos.

Os riscos identificados serão avaliados quanto ao seu potencial impacto e, quando necessário, serão definidas medidas para sua mitigação, acompanhamento ou aceitação pela administração.

A Gestora manterá registros das avaliações realizadas e das medidas adotadas para o tratamento dos riscos identificados.

Quando aplicável, a avaliação poderá contemplar riscos relacionados a serviços em nuvem, fornecedores críticos, proteção de dados pessoais, ativos digitais e demais recursos tecnológicos utilizados em suas atividades.

A avaliação dos riscos e as ações de prevenção inerentes às atividades desempenhadas pela Genesis Capital estão descritas no Anexo II da presente Política.

.

A avaliação dos riscos e as ações de prevenção inerentes às atividades desempenhadas pela Genesis Capital estão descritas no Anexo II da presente Política.

(i) Ações de Prevenção e Proteção

Todo o procedimento operacional é monitorado pela Empresa de TI Terceirizada contratada.

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para Gestora, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Genesis Capital, em caso de incidente de segurança.

Deste modo, a Genesis Capital segrega as informações geradas pela Gestora, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Assim, classifica-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag*:

- Quaisquer informações e/ou dados que a Gestora teve acesso ou conhecimento por ser de domínio público (“Informação Pública”);
- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) *Yellow Flag*:

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) *Red Flag*:

- Todas as Informações Confidenciais, a saber:
    - know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela Genesis Capital;
    - operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Genesis Capital; e
    - estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Genesis Capital e/ou de seus sócios e clientes.

A partir da definição acima, a Genesis Capital se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: Red Flag, Yellow Flag e Green Flag. Todos os Colaboradores, ao tomarem conhecimento de qualquer incidente referente à segurança da informação e cibernética, devem notificar o fato, imediatamente ao Compliance, via e-mail.

A partir desse ponto, passamos a mencionar os procedimentos de prevenção e proteção adotados pela Gestora:

1. Propriedade dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da Genesis Capital.

A utilização de dispositivos pessoais (BYOD) para atividades da Gestora dependerá de autorização da Diretoria de Compliance e do atendimento às medidas básicas de segurança definidas pela empresa. A Gestora poderá restringir ou revogar acessos sempre que identificar riscos à segurança de suas informações.

2. Disponibilização e uso

Todos os computadores disponibilizados para os Colaboradores da Genesis Capital têm por objetivo o desempenho das atividades profissionais na Gestora, não devendo ser utilizado para quaisquer outros fins.

Conforme anteriormente citado, todo o processo de criação e exclusão de usuário, instalação de *softwares* e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela Empresa de TI Terceirizada, mediante aprovação do Diretor de *Compliance*.

A disponibilização e uso dos computadores da Genesis Capital respeitam as seguintes regras:

- A cada novo Colaborador, o Diretor de *Compliance* autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela Empresa de TI Terceirizada, mediante supervisão e aprovação do Diretor de *Compliance*.
- o Diretor de *Compliance* autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade Empresa de TI Terceirizada, mediante supervisão e aprovação do Diretor de *Compliance*.
- A identificação do usuário é feita através do *login* e senha, que através do registro de logs utilizado pela Genesis Capital é sua assinatura eletrônica no servidor da Gestora.

  Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela Genesis Capital, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue.
- É permitido apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação ao Diretor de *Compliance*.
- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da respectiva expiração..

- Todos os eventos de *login* e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pelo Diretor de *Compliance*.

3. *Softwares*

A implantação e configuração de *softwares* na Genesis Capital respeitam as seguintes regras:

- Todos os *softwares*, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela Empresa de TI Terceirizada, mediante supervisão e aprovação do Diretor de *Compliance.*
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada do Diretor de *Compliance*.
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores.
- Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Gestora.
- A utilização de equipamentos pessoais por terceiros nas instalações da Gestora e a conexão destes na rede interna à Internet requer autorização prévia e expressa do Diretor de *Compliance*. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.
- A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia e expressa do Diretor de *Compliance*.

4. Gestão de Vulnerabilidades e Atualizações de Segurança

- A Genesis Capital adotará processo formal de gestão de vulnerabilidades e atualização de segurança de sistemas, aplicações, equipamentos e demais ativos tecnológicos relevantes.
- As atualizações críticas de segurança disponibilizadas pelos fornecedores deverão ser avaliadas, testadas em ambiente de homologação e implementadas em prazo não superior a 90 (noventa) dias, salvo justificativa técnica formal.
- Caso a atualização não seja considerada aplicável ou sua implementação represente risco operacional relevante, deverá ser formalizada justificativa

contendo análise de risco, medidas compensatórias adotadas e aprovação do Compliance.

- A Empresa de TI Terceirizada realizará monitoramento contínuo de vulnerabilidades identificadas em sistemas, aplicações e infraestrutura tecnológica da Gestora, propondo medidas de remediação compatíveis com a criticidade dos riscos identificados.

5. Identificação de Atividades Maliciosas

- A Genesis Capital manterá processos e controles destinados à identificação tempestiva de atores maliciosos, comportamentos suspeitos, acessos indevidos, comprometimento de credenciais, dispositivos não autorizados e demais eventos que possam representar risco à segurança cibernética, à integridade das informações, aos dados pessoais tratados ou à integridade dos mercados em que atua.

- Para esse fim, poderão ser utilizados mecanismos de monitoramento de logs, eventos de autenticação, trilhas de auditoria, alertas de segurança, relatórios de vulnerabilidades e demais ferramentas de supervisão tecnológica, sob responsabilidade da Empresa de TI Terceirizada e supervisão do Compliance.

6. Registros

A Genesis Capital deve manter por 05 (cinco) anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados.

Nesse sentido, através dos logs realizados pela Gestora, a Genesis Capital consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme 4º, §8º, da Resolução CVM nº 21/21.

7. Responsabilidades do usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela Genesis Capital.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;

- Não transportar Informações Confidenciais da Genesis Capital em qualquer meio (CD, DVD, *pendrive*, papel etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos que contêm Informações Confidenciais; e
- Seguir corretamente a política para uso de internet e correio eletrônico estabelecida pela Genesis Capital.

8. Outras Proteções aos Computadores

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente).
- "*Log-off*" automático por inatividade durante o período de 24 horas.
- Bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores.
- Bloqueio do acesso a sites de armazenamento de dados em Nuvem (*Cloud Service*) não aprovados pelo Comitê de Compliance.
- Bloqueio de sistemas de gerenciamento de computador à distância.

9. Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia da Genesis Capital, este deve sempre resguardar a imagem da Gestora, evitando entrar em sites de fontes não seguras, assim como de abrir e-mails pessoais, ou, de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pelo Diretor de *Compliance*.

O usuário é proibido de acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (*softwares*) ou patentes existentes.
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.

- Contenham informações que não colaborem para o alcance dos objetivos da Genesis Capital.
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

É proibido o uso de serviços de mensagem instantânea (MSN, Skype etc), através dos computadores da Genesis Capital, exceto em eventuais situações de uso profissional, sendo necessária autorização do Diretor de *Compliance*.

Também se faz expressamente proibido o uso de serviços de rádio, *streaming*, *download* de vídeos, filmes e músicas, através dos computadores da Genesis Capital.

10. Bloqueio de endereços de Internet

Periodicamente, o *Compliance* irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética Corporativa da Gestora.

11. Uso de correio eletrônico particular

É proibido a utilização profissional de correio eletrônico particular.

A Genesis Capital disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@genesiscapital.com.br). O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à Gestora.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Genesis Capital.

Se houver necessidade de troca de endereço, a alteração será realizada pela Empresa de TI Terceirizada, mediante autorização e supervisão do Diretor de *Compliance*.

12. Endereço eletrônico de programas ou de comunicação corporativa

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da

Área de *Compliance* responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da Genesis Capital, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas ao respectivo correio eletrônico são de propriedade da Genesis Capital.

13. Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela Genesis Capital mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da Genesis Capital.

14. Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, podendo enviar mensagens necessárias para o seu desempenho profissional na Gestora.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Gestora, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;

- Defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da Genesis Capital; e
- Sejam incoerentes com o Código de Ética Corporativa da Genesis Capital.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da Genesis Capital é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da Genesis Capital.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo respectiva confidencialidade; e
- Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

15. Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria a cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da Empresa de TI Terceirizada, mediante supervisão do Diretor de

Compliance.

16. Armazenamento em Nuvem (*Cloud*)

A Genesis Capital realiza o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (*Cloud Service*).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

Fornecedores, prestadores de serviços e parceiros ("Terceiros") podem representar uma fonte significativa de riscos para a Genesis Capital em relação à *Cibersegurança*. Neste sentido, necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de Armazenamento em Nuvem.

Necessário iniciar um devido processo de *Due Diligence* do Terceiro antes da contratação, devendo-se constatar se a organização segue políticas, programas e procedimentos formais relativos à segurança da informação e *Cibersegurança*.

Com isto em mente, a empresa objeto de contratação deverá enviar a Gestora:

(i) Documentos que atestem a existência dos respectivos procedimentos de *Cibersegurança*;
(ii) Último relatório de teste/auditoria periódica; e
(iii) As certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

Uma vez recebidos os respectivos documentos, o *Compliance* analisará o Terceiro, podendo negar de imediato a contratação deste ou exigir remediações para que este se encaixe nos moldes de segurança a serem aplicados pela Gestora.

Somente após a aprovação pelo *Compliance*, o Terceiro poderá ser contratado para prestar serviços de Armazenamento na Nuvem.

Em caso de qualquer incidente constatado pelo Terceiro, este deverá de imediato enviar uma notificação relatando o ocorrido à Genesis Capital, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos de *Due Dilligence* aos provedores destes serviços.

17. Contratação de Serviços de Processamento e Armazenamento de Dados em Nuvem

A Genesis Capital irá verificar a capacidade e o potencial prestador de serviço, na contratação de serviços de processamento e armazenamento de dados em nuvem, incluindo, no mínimo:

(i) O acesso da Genesis Capital aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

(ii) A confidencialidade, a integridade, a disponibilidade e a recuperação das informações e dados processados ou armazenados pelo prestador de serviço;

(iii) A sua aderência a certificações exigidas pela Genesis Capital ou reguladores para a prestação do serviço a ser contratado, caso aplicável;

(iv) O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

(v) A identificação e a segregação dos dados dos clientes, funcionários, colaboradores ou terceiros relevantes por meio de controles físicos ou lógicos;

(vi) A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes, funcionários, colaboradores e terceiros relevantes.

(vii) Adicionalmente, a Genesis Capital poderá utilizar o questionário de *Due Diligence* para contratação de serviço de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, disponibilizado no site da ANBIMA.

18. Destruição de Documentos

Descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

XII. 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, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Genesis Capital, 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.

O Colaborador, deverá assinar o Termo de Adesão da Genesis Capital, conforme Anexo I da presente política.

XIII. USO DE EQUIPAMENTOS, SISTEMAS, SEGURANÇA E CONFIDENCIALIDADE

Os acessos físicos são controlados pelo Compliance e orientados de forma a garantir que apenas pessoas autorizadas possuam o efetivo acesso às instalações e equipamentos que pertençam e/ou que sejam utilizados pela Gestora.

Os acessos às informações (dados) e aos ambientes lógicos (sistemas) são controlados, de forma a garantir o efetivo acesso apenas de pessoas autorizadas, sendo certo que tal restrição/segregação será feita em relação a: (i) área/atividade, (iii) cargo/nível hierárquico e (iii) equipe.

Cada colaborador e terceiro contratado é responsável por manter o controle e sigilo de todas os tipos de informações da Genesis Capital, citados nesta política, bem como em especial atenção para as informações confidenciais e privilegiadas que lhes tenham sido confiadas em virtude do exercício de suas atividades profissionais, excetuadas as hipóteses permitidas em lei e que estão sob sua responsabilidade.

Conforme estabelecido pela Genesis Capital, todos os Colaboradores e terceiros contratados devem assinar, de forma manual ou eletrônica, o Termo de Adesão, constante no Anexo I desta Política, comprometendo-se a observar integralmente os termos desta Política de Segurança da Informação e Segurança Cibernética.

Estão dispensados de assinar o Termo de Adesão os terceiros contratados, que em seu contrato de prestação de serviço haja uma cláusula de confidencialidade.

A Genesis Capital possui uma Política de Segregação e Confidencialidade, em que reafirma e trata o compromisso da Gestora com os princípios da ética, transparência, segurança e respeito, com o adequado gerenciamento, acesso e preservação das informações confidenciais e privilegiadas de sua propriedade ou sob a guarda da Genesis Capital.

A Política de Segregação e Confidencialidade é um documento independente, porém integrante a esta Política de Segurança da Informação e Segurança Cibernética e nela todos os colaboradores e terceiros contratados possam verificar com maior detalhamento o tema abordado.

XIV. PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a Genesis Capital desenvolveu um Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na ocorrência de incidente de segurança da informação ou segurança cibernética, inclusive em decorrência de crimes cibernéticos, a Diretoria de Compliance e os responsáveis envolvidos avaliarão o caso e adotarão as medidas cabíveis, podendo o assunto ser submetido ao Comitê Único ("Comitê"), quando necessário.

Em caso de incidente relevante de segurança da informação ou segurança cibernética, a Diretoria de Compliance e os responsáveis envolvidos avaliarão, conforme aplicável: (i) a natureza e a gravidade do incidente; (ii) seus potenciais impactos; (iii) a necessidade de adoção de medidas de contingência e continuidade dos negócios; (iv) a realização de comunicações a clientes, titulares de dados, reguladores e autoridades competentes; (v) o acompanhamento das ações de correção e recuperação; e (vi) o encerramento formal do incidente.

Os incidentes de segurança da informação e segurança cibernética serão avaliados conforme sua relevância e potenciais impactos operacionais, financeiros, regulatórios e reputacionais.

Quando exigido pela legislação, regulamentação ou obrigações contratuais, a Gestora realizará as comunicações cabíveis aos clientes, reguladores, autoridades competentes, titulares de dados pessoais ou demais partes afetadas.

A Gestora manterá registro dos incidentes identificados, das avaliações realizadas e das medidas adotadas para sua contenção, correção e eventual comunicação, observados os prazos legais e regulatórios aplicáveis. Estas providências consistem em:

Empresa de TI Terceirizada (Sob Supervisão do *Compliance*):

a) Verificação e Auditoria dos Logs;

b) Criação de laudo pericial contendo as informações que foram potencialmente vazadas;

c) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;

d) Desinstalação de *software*;

e) Execução de varreduras *offline* para descobrir quaisquer ameaças adicionais;

f) Formatação e reconstrução do sistema operacional;

g) Substituição física de dispositivos de armazenamento;

h) Reconstrução de sistemas e redes;

i) Restauração de dados provenientes do *backup* realizado diariamente; e

j) Entre outros.

Compliance ou Jurídico Contratado:

a) Criação de relatório baseado no laudo pericial elaborado pela Empresa de TI Terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança.

b) Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido.

Encarregado de Dados:

a) Caso o incidente envolva dados pessoais e possa acarretar risco ou dano relevante aos titulares, a Genesis Capital comunicará a Agência Nacional de Proteção de Dados (ANPD) e os titulares afetados; observando os requisitos legais e regulatórios e o prazo de até 3 (três) dias úteis contados do conhecimento da ocorrência.

BackOffice:

a) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Companhia.

b) Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos da Gestora resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados pelo Compliance, bem como ser formalizado no Relatório de Controles Internos da Genesis Capital.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da Genesis Capital.

XV. PROTEÇÃO DE DADOS

Todos os Dados Pessoais que a Genesis Capital mantiver contato, seja como controladora ou operadora perante a classificação da Lei Geral de Proteção de Dados (Lei nº 13.709) serão classificadas como Informação Confidencial e deverão obedecer às premissas da Política de LGPD da Genesis Capital. Todo Dado Pessoal que não tiver embasamento legal para ser tratado ou armazenado deverá ser excluído.

Os critérios próprios, as regras e procedimentos que tratem da privacidade e dos dados pessoais a que a Genesis Capital tenha acesso, está descrito em um documento independente, porém integrante a esta Política de Segurança da Informação e Segurança Cibernética e nela todos os colaboradores e terceiros contratados possam verificar com maior detalhamento o tema abordado.

Qualquer solicitação em relação ao tratamento de dados pessoais ou de informações específicas relacionadas ao tratamento de dados pessoais, deverá ocorrer por meio do e-mailri@genesiscapital.com.br.

A Genesis Capital observará os requisitos da Lei Geral de Proteção de Dados (LGPD) e demais normas aplicáveis à proteção de dados pessoais, adotando medidas de governança, segurança e privacidade compatíveis com a natureza de suas atividades.

A Gestora manterá controles e registros relacionados ao tratamento de dados pessoais, incluindo, quando aplicável, o mapeamento das operações de tratamento, a gestão dos direitos dos titulares e a avaliação de riscos à privacidade.

O Encarregado pelo Tratamento de Dados Pessoais atuará de forma independente no exercício de suas atribuições, devendo eventuais conflitos de interesse ser identificados e tratados pela Gestora.

As transferências internacionais de dados pessoais, quando realizadas, deverão observar os requisitos previstos na legislação e regulamentação aplicáveis.

XVI. MONITORAMENTO E TESTES DE CONTINGÊNCIA

A Genesis Capital manterá mecanismos de acompanhamento destinados a assegurar a implementação e efetividade desta Política.

Os controles incluirão, quando aplicável: (i) monitoramento de incidentes; (ii) monitoramento de acessos; (iii) análise de logs; (iv) monitoramento de vulnerabilidades; (vi) monitoramento de terceiros críticos; (v) acompanhamento da execução de backups.

Serão adotados indicadores de desempenho (KPIs), incluindo: (i) quantidade de incidentes; (ii) tempo médio de resposta; (iii) percentual de conclusão dos treinamentos; (iv) percentual de vulnerabilidades corrigidas; e (v) resultado dos testes realizados.

Anualmente serão realizados testes de segurança e continuidade, incluindo, conforme aplicável: (i) testes de restauração de backup; (ii) tabletop exercise; (iii) testes de phishing; (iv) testes de resposta a incidentes; (v) análise de vulnerabilidades; e (vi) testes de intrusão (pentest).

Os resultados deverão ser documentados, avaliados pelo Compliance e acompanhados por plano de ação corretivo.

XVII. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE AMEAÇAS E INCIDENTES CIBERNÉTICOS

A Genesis Capital poderá participar de iniciativas e fóruns voltados ao compartilhamento de informações sobre segurança cibernética, com o objetivo de fortalecer seus controles e sua resiliência operacional. Eventuais compartilhamentos deverão observar os deveres de confidencialidade, a proteção de dados pessoais e as disposições legais e regulatórias aplicáveis.

A Gestora realizará testes periódicos de seus procedimentos de continuidade de negócios, conforme previsto em seu Plano de Continuidade de Negócios, com o objetivo de verificar sua capacidade de resposta a incidentes e de manter a continuidade de suas atividades.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Genesis Capital esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da Genesis Capital.

XVIII. DIVULGAÇÃO

A Política de Segurança da Informação e Segurança Cibernética, normas e procedimentos relativos ao tratamento dos ativos de informação e/ou dados sigilosos são apresentados aos Colaboradores, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento. A presente Política será divulgada por intermédio de mensagem eletrônica (e-mail), assim como estará disponível em um diretório interno da Genesis Capital, com total acesso a todos os colaboradores e terceiros contratados.

XIX. MANUTENÇÃO DOS ARQUIVOS

A Genesis Capital manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Compliance desta política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

Além disso, a Gestora manterá registros de eventos e incidentes de segurança da informação, quando aplicável, para auxiliar no monitoramento de riscos e na adoção de medidas preventivas e corretivas.

XX. CONSIDERAÇÕES FINAIS

O dever de sigilo não impede o compartilhamento de informações e documentos com reguladores, autorreguladores e autoridades competentes, quando exigido pela legislação, regulamentação ou normas aplicáveis.

Esta Política deverá ser interpretada em conjunto com as demais políticas e procedimentos internos da Genesis Capital relacionados à segurança da informação, proteção de dados e continuidade dos negócios.

Qualquer situação que indique a suspeita ou a confirmação de ocorrência de incidente de segurança deve ser reportada imediatamente à Diretoria de Compliance.

Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com o Compliance da Genesis Capital.

Rua Iguatemi, 448 | 6º andar
Itaim Bibi | CEP: 01451-010
Tel.: 11 4993-9400

ANEXO I – TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/MF sob o nº _____, declaro que recebi, li e compreendi a **Política de Segurança da Informação e Segurança Cibernética da Genesis Capital Gestora de Recursos Ltda.**, comprometendo-me a cumprir integralmente suas diretrizes e demais normas internas relacionadas à segurança da informação, privacidade e proteção de dados.

Comprometo-me a:

- Utilizar as informações, sistemas, equipamentos e demais recursos tecnológicos da Gestora exclusivamente para fins profissionais autorizados;
- Preservar a confidencialidade, integridade e disponibilidade das informações às quais tiver acesso em razão das minhas atividades;
- Manter sigilo sobre informações confidenciais, restritas ou privilegiadas da Gestora, de seus clientes, parceiros e prestadores de serviços, inclusive após o encerramento do meu vínculo com a empresa;
- Observar as diretrizes internas relacionadas à privacidade e proteção de dados pessoais, em conformidade com a legislação aplicável;
- Comunicar imediatamente à Diretoria de Compliance qualquer incidente, suspeita de incidente, perda de equipamento, acesso não autorizado, vazamento de informações ou qualquer situação que possa representar risco à segurança da informação, à segurança cibernética ou à proteção de dados;
- Participar dos treinamentos e ações de conscientização promovidos pela Gestora, quando aplicáveis.

Declaro estar ciente de que o descumprimento das disposições da Política de Segurança da Informação e Segurança Cibernética, das normas internas da Gestora ou da legislação aplicável poderá sujeitar-me às medidas disciplinares e legais cabíveis.

Por fim, declaro estar de acordo com todas as disposições acima e assumo o compromisso de observá-las durante todo o período de meu vínculo com a Genesis Capital Gestora de Recursos Ltda.

São Paulo, [Data]

_____

[Assinatura]

Rua Iguatemi, 448 | 6º andar
Itaim Bibi | CEP: 01451-010
Tel.: 11 4993-9400

ANEXO II – MATRIZ DE AVALIAÇÃO DE RISCOS CIBERNÉTICOS E SEGURANÇA DA INFORMAÇÃO

A Matriz de Riscos tem caráter orientativo e servirá como instrumento de apoio para a identificação, avaliação, tratamento e monitoramento dos riscos relacionados à Segurança da Informação, Segurança Cibernética, Privacidade e Proteção de Dados.

Os riscos identificados deverão ser avaliados periodicamente e sempre que houver alterações relevantes nos processos, sistemas, tecnologias ou prestadores de serviços da Gestora.

Os riscos poderão ser classificados de acordo com seu potencial impacto e probabilidade de ocorrência, sendo definidas, quando necessário, medidas para sua mitigação, transferência, aceitação ou eliminação.

A aceitação de riscos considerados relevantes deverá ser avaliada pela Diretoria da Gestora.

Com base nos processos, sistemas e ativos utilizados em suas atividades, a Genesis Capital avaliará os riscos aplicáveis e adotará medidas de prevenção e proteção compatíveis com seu porte, estrutura e perfil de risco, assim, as correspondentes ações de prevenção e proteção, conforme mapeamento abaixo:

Ativo / Processo	Ameaça	Impacto Potencial	Nível de Exposição	Principais Controles
Correio eletrônico corporativo	Phishing, comprometimento de credenciais, malware	Operacional, regulatório e reputacional	Alto	MFA, filtros antispam, monitoramento de acessos, treinamento periódico e campanhas de conscientização
Ambiente de nuvem	Acesso indevido, indisponibilidade, vazamento de dados	Operacional, financeiro e regulatório	Alto	Due diligence de fornecedores, MFA, criptografia, backup e monitoramento contínuo
Dados pessoais	Vazamento, acesso não autorizado, exclusão indevida	Regulatório, financeiro e reputacional	Alto	Controle de acesso, segregação de funções, rastreabilidade, criptografia e monitoramento
Sistemas corporativos	Malware, ransomware, exploração de vulnerabilidades	Operacional e financeiro	Alto	Gestão de vulnerabilidades, antivírus, atualização de segurança e backups testados
Equipamentos corporativos	Furto, perda, acesso indevido	Operacional e reputacional	Médio	Criptografia, bloqueio automático de tela e gerenciamento centralizado
Informações Confidenciais e Restritas	Divulgação indevida	Regulatório, financeiro e reputacional	Alto	Classificação da informação, Need to Know e controle de acessos
Prestadores de serviços críticos	Falha operacional ou incidente cibernético	Operacional, regulatório e financeiro	Alto	Due diligence, monitoramento contínuo, cláusulas contratuais e avaliações periódicas
Ambiente de trading e investimentos	Engenharia social, fraude operacional	Financeiro e reputacional	Alto	Dupla verificação, segregação de funções, monitoramento de operações e registros auditáveis

Infraestrutura tecnológica	Ataques DDoS, indisponibilidade de serviços	Operacional	Médio	Redundância, monitoramento, plano de continuidade e testes periódicos
Bases de dados e arquivos eletrônicos	Corrupção, perda ou exclusão indevida	Operacional e regulatório	Alto	Backup, recuperação testada, controle de acesso e monitoramento