COMPOSTELA

POLÍTICA DE GOVERNANÇA EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

COMPOSTELA CAPITAL GESTORA DE RECURSOS LTDA.

SUMÁRIO

I. OBJETIVO 3
II. ABRANGÊNCIA 3
III. PÚBLICO ALVO 3
IV. REVISÃO E ATUALIZAÇÃO 4
V. DEFINIÇÕES 4
VI. PRINCÍPIOS 7
VII. DIRETRIZES 10
VIII. DADOS PESSOAIS SUJEITOS À ESTA POLÍTICA 12
IX. TRATAMENTO DOS DADOS COLETADOS 13
X. BOAS PRÁTICAS DE UTILIZAÇÃO 14
XI. BLOQUEIO DE ACESSO A SITES 14
XII. SITES DE ARMAZENAMENTOS DE ARQUIVOS 15
XIII. GESTÃO DE RISCOS, TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO, CONTINUIDADE DE NEGÓCIO E BACKUPS 15
XIV. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA 16
XV. AÇÕES DE PREVENÇÃO E PROTEÇÃO 17
XVI. PLANO DE RESPOSTA 19
XVII. RECICLAGEM E REVISÃO 20
XVIII. TESTES DE CONTROLES 20
XIX. VEDAÇÕES 21
XX. PROPRIEDADE INTELECTUAL 22
XXI. RASTREAMENTO 22
XXII. DESCUMPRIMENTO 22
XXIII. TERMO DE CONHECIMENTO 23

I. OBJETIVO

Formalizar os procedimentos e diretrizes para gerenciamento de privacidade e segurança da informação na Compostela Capital GESTORA de Recursos Ltda (“GESTORA” ou “COMPOSTELA”)

II. ABRANGÊNCIA

Esta Política é aplicável à GESTORA e a todos os que tenham acesso a quaisquer dados pessoais detidos por ela ou em nome dela (“pessoas abrangidas”), e visa proteger os direitos dos titulares de quaisquer operações de tratamento de dados pessoais tratados em seu ambiente corporativo e no ambiente corporativo de terceiros.

Cabe a GESTORA e seus colaboradores atender às diretrizes e procedimentos estabelecidos nesta Política de Governança em Privacidade e Segurança da Informação (“Política”), informando quaisquer irregularidades à Diretora de Compliance e de Gestão de Risco, a quem caberá avaliá-las e submetê-las ao Comitê de Compliance, Controles Internos e Ética, o qual decidirá sobre eventuais medidas cabíveis.

A Diretora de Compliance e de Gestão de Risco deve garantir o seguimento desta Política, sendo o responsável por temas de segurança da informação e cibernética da GESTORA. Eventual conflito entre legislação e esta Política deverá prevalecer a legislação.

III. PÚBLICO ALVO

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta, das atividades diárias e negócios, representando a GESTORA (doravante, “Colaboradores”).

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade à Diretora de *Compliance* e de

Gestão de Risco (“Diretora de *Compliance* e de Gestão de Risco e/ou Diretora responsável”).

IV. REVISÃO E ATUALIZAÇÃO

Esta Política deverá ser revisada e atualizada a cada 12 (doze) meses, ou em prazo inferior, caso necessário, em função de mudanças legais, regulatórias, autorregulatória ou complementações.

Este documento revoga todas as versões anteriores e passa a vigorar na data de sua aprovação.

A área de Compliance informará oportunamente aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da GESTORA na rede mundial de computadores.

V. DEFINIÇÕES

Para efeito desta política são adotadas as seguintes definições:

Conformidade: Cumprimento de leis, regulamentos, normas técnicas e instrumentos jurídicos;

Informação: Dados, processados ou não, contidos em qualquer meio, suporte ou formato, que podem ser utilizados para produção e transmissão de conhecimento;

Informação Confidencial: informação a qual o acesso, divulgação, reprodução são restritas pela lei, regulamento, política interna ou derivado de obrigação contratual;

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável - aquela que pode ser reconhecida, direta ou indiretamente, a partir de um identificador como um nome, número de identificação, dados de localização, identificador online ou um ou mais fatores específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural;

Dado pessoal sensível: referente a 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;

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Integridade: Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

Riscos de segurança da informação: Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo nas atividades da GESTORA;

Segurança da informação: Ações que objetivam viabilizar e assegurar o sigilo, integridade, autenticidade, disponibilidade e conformidade de dados e informações;

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Ex. nossos colaboradores;

Encarregado: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), Ex. Diretora de Compliance;

Agentes de tratamento: O controlador e o operador;

Tratamento: Toda operação realizada com dados pessoais, desde a recepção e/ou coleta, produção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Eliminação: Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Autoridade nacional: Autoridade Nacional de Proteção de Dados (ANDP) órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

São consideradas "Informações Confidenciais" aquelas não disponíveis ao público, que:

- Identifiquem dados pessoais, patrimoniais ou estratégicos;

- Sejam objeto de acordo de confidencialidade celebrado com terceiros;

- Identifiquem ações estratégicas – dos negócios da empresa, seus clientes ou dos portfólios sob gestão – cuja divulgação possa prejudicar a gestão dos negócios, clientes e fundos de investimentos geridos pela GESTORA, ou reduzir sua vantagem competitiva;

- Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente que digam respeito às atividades da GESTORA e que sejam devidamente identificadas como sendo confidenciais, constituam propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;

- Sejam assim consideradas face a determinação legal, previsão legal e/ou regulamentar;

- O Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás) de uso pessoal e intransferível.

Na atividade de gestão, a GESTORA considera que o controle do fluxo de informações é o risco mais relevante em termos de controle estratégico para o negócio. A mitigação de tal risco se dá através de procedimentos operacionais de segurança, ligados ao uso de equipamentos internos (mitigado através dos contratos/sistemas fornecidos pelos prestadores de serviço), e, através de procedimentos internos que parametrizam o comportamento dos Colaboradores, descritos neste documento.

Em caso de dúvida, o Colaborador deverá consultar previamente a Diretora de Compliance e de Gestão de Risco acerca da possibilidade de compartilhamento da Informação Confidencial, a qual deverá se manifestar formalmente sobre o caso.

VI. PRINCÍPIOS

Esta política visa fortalecer os mecanismos de geração, recepção, organização, tratamento, acesso, preservação, recuperação, divulgação, compartilhamento, reuso e eliminação das informações necessárias à consecução da atividade da GESTORA.

A política tem como premissa que dados e informações organizados, documentados, acessíveis e verificados quanto a sua exatidão e validade são essenciais para a prevenção de fraudes, mitigação do risco de incidentes de divulgação indevida de informações, garantir o sigilo, integridade, autenticidade, disponibilidade, conformidade e segurança de dados e informações.

A gestão de dados, informação e conhecimento na GESTORA tem como princípios norteadores:

- **Confidencialidade**: O acesso à informação deve ser obtido somente por pessoas autorizadas, e quando ele for de fato necessário;

- **Disponibilidade**: Os agentes de tratamento devem ter acesso à informação sempre que necessário;

- **Dados, informação e conhecimento como ativos corporativos**: Dados, informação e conhecimento produzidos no exercício das funções da GESTORA são de propriedade da Empresa e serão gerenciados como ativos corporativos;

- **Prevenção:** A gestão de dados e informação e do conhecimento, estará pautada pela legislação vigente e atuará de modo a identificar, avaliar e tratar potenciais riscos institucionais e de segurança da informação, adotando medidas necessárias para prevenir a ocorrência de danos;

- **Adequação:** O tratamento dos dados e informação deverá se ater estritamente ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos, de acordo com o contexto do tratamento.

- **Preservação**: Dados, informações e conhecimento produzidos pela GESTORA serão armazenados e preservados a longo prazo, sempre que possível e justificável, para resguardar a memória técnica e institucional;

- **Privacidade**: A GESTORA atuará de modo a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, promovendo boas práticas de governança e gestão, para construção de uma relação de confiança com o cidadão e em respeito à legislação nacional de proteção de dados pessoais;

- **Segurança**: Os dados e informações serão protegidos para garantia do sigilo devido e de sua integridade, autenticidade, disponibilidade e conformidade. Instrumentos normativos específicos e medidas de proteção contra perda intencional ou não, destruição, modificação e

acesso não autorizados serão estabelecidos em atendimento à legislação vigente;

- **Transparência**: A GESTORA assegura aos titulares dos dados o livre e facilitado acesso acerca da realização do tratamento, os respectivos agentes de tratamento, fornecendo informações claras e precisas, resguardados os sigilos comerciais;

- **Não discriminação**: Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares;

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da GESTORA:

- As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;

- A informação deve ser utilizada de forma transparente, e apenas para a finalidade para a qual foi coletada;

- A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades. Desta forma, há a segregação lógica das informações, de modo que somente os Colaboradores autorizados têm acesso às pastas virtuais respectivas às suas atividades desenvolvidas na GESTORA;

- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

- Segregação de instalações, equipamentos e informações comuns, quando aplicável;

- A senha de acesso à rede e caixas de e-mails deverão ser utilizadas como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados imediatamente à Diretora de Compliance e de Gestão de Risco.

VII. DIRETRIZES

Para assegurar que as informações e dados pessoais sejam adequadamente protegidas, a GESTORA definiu os seguintes processos/controles:

- Monitoramento de contas de usuário privilegiados, com inspeção de conteúdo e registro de tipo de uso dos e-mails feitos pelos usuários a qualquer tempo;

- Monitoramento do acesso e uso de bancos de dados com dados pessoais;

- Implementação de *hardening* de servidores;

- Encriptação de dados pessoais e dados pessoais sensíveis;

- Uso de autenticação multifatorial;

- Controle de acesso rígido para aplicações, com base na necessidade e remoção de acesso quando não for mais necessário;

- Teste de invasão realizado trimestralmente;

- Não armazenamento de senhas em texto claro em arquivos não criptografados;

- Registro de tentativas de identificação do usuário para acesso ao sistema sem sucesso;

- Revisão anual de códigos para verificação se há dados pessoais indevidos;

- Exclusão dos Dados Pessoais em arquivo eletrônico ao final do tratamento dos dados ou solicitação do titular;

- Destruição de Informação Confidencial ou dados pessoais armazenados em meio físico efetuado utilizando máquina fragmentadora de papéis;

- Não deixar à vista nos locais de trabalho nenhuma Informação Confidencial, ou abandonar documento impresso em equipamento coletivo;

- Bloquear a estação de trabalho sempre que se ausentar do seu local de trabalho, mesmo que temporariamente;

- Desligar o equipamento no final do expediente;

- Utilizar exclusivamente os meios de comunicação reconhecidos pela GESTORA, em mensagens escritas sempre que aplicável, quais sejam: Microsoft Outlook para e-mails, Microsoft SharePoint com acesso as pastas e arquivos, Microsoft OneDrive para guarda e compartilhamento de arquivos, Microsoft Teams para mensagens instantâneas, ramal de telefone corporativo;

- O uso de chat do Skype é admitido para emissão de ordem com as corretoras de títulos e valores mobiliários, desde que a mensagem seja escrita, não se admitindo mensagens de áudio;

- Disponibilizar esses recursos a terceiros, caso entenda necessário;

- Utilização de GS Wave App. Aplicativo para dispositivos móveis para ligações institucionais, apenas em caráter de exceção;

- Adoção de boas práticas, ações de prevenção e proteção e bloqueio de "imitações" do domínio, a fim de evitar fraudes enviadas por e-mail;

- Adoção de Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e Backups, Procedimentos de Segurança Cibernética, Plano de resposta, Revisão e Reciclagem, e Testes de Controles.

- Bloqueio de acesso a sites proibidos;

- Utilização de Control ID (Biometria);

- Utilização de Multifuncionais (Livro de endereços para digitalização em rede);

- Utilização de WiFi com Registro do IP dos dispositivos que acessarão;

- Registro de identificação de usuário para acesso ao Windows;

- Implementação do Antivírus em dispositivos móveis - Kaspersky;

- Implementação da Política de Consentimento de Privacidade;

- Imediata adaptação ou cancelamento da senha de acesso do colaborador em caso de mudança de área ou desligamento, visando ao impedimento de acesso não autorizado pelo antigo Colaborador;

- Descarte imediato dos dados pessoais sensíveis diante do desligamento de Colaboradores.

VIII. DADOS PESSOAIS SUJEITOS À ESTA POLÍTICA

Estão sujeitos à esta Política, todos os dados pessoais fornecidos pelos participantes e tratados pela GESTORA, no contexto da prestação dos serviços realizada em seus sistemas, todos os dados pessoais tratados pela GESTORA, no contexto do seu sítio eletrônico.

Todos os dados pessoais de empregados, colaboradores, administradores, acionistas prestadores de serviços, parceiros e clientes, tratados pela GESTORA, no contexto de obrigação contratual, societária ou legal.

IX. TRATAMENTO DOS DADOS COLETADOS

Os dados pessoais serão tratados, conforme o caso, de forma transparente, ética e nos termos e limites da legislação em vigor, em ambiente robusto, seguro e controlado, pelo prazo exigido na regulamentação vigente.

A GESTORA adota todas as medidas cabíveis e boas práticas de utilização dos dados para manter o absoluto sigilo e a estrita confidencialidade de todos os dados pessoais a que tiver acesso.

O acesso dos dados pessoais por parte de terceiros poderá se dar: (i) em atendimento à legislação em vigor; (ii) em atendimento aos órgãos reguladores; e (iii) em atendimento à auditoria interna e auditores independentes.

A GESTORA manterá armazenados os dados pessoais, nos termos da legislação e regulamentação em vigor, e exclusivamente para o atendimento de finalidades específicas pretendidas.

Ao final do tratamento, os dados utilizados serão mantidos em área com acesso restrito à equipe jurídica e de Compliance da GESTORA.

Os dados utilizados em operações e negócios entabulados pela GESTORA no exercício de sua atividade, em seu próprio nome ou em nome de algum dos fundos de investimento por ela gerido, serão mantidos por até 10 (dez) anos antes de seu efetivo descarte/exclusão para fins de Compliance, obrigações legais ou processo de “Know Your Client”.

Os dados coletados para análise para estruturação de eventuais operações não efetivamente concretizadas, serão armazenadas por até 05 (cinco) anos antes de seu efetivo descarte/exclusão.

Os dados coletados pelo sítio eletrônico da GESTORA mediante fornecimento de consentimento poderão ser imediatamente excluídos mediante solicitação do titular.

X. BOAS PRÁTICAS DE UTILIZAÇÃO

A utilização da rede, internet, e-mail e dispositivos móveis na GESTORA e/ou pelos seus Colaboradores em comunicações de trabalho devem se dar pelas seguintes regras:

- Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- Somente imprimir as mensagens quando realmente necessário;
- Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abri-la, para evitar vírus ou códigos maliciosos;
- No caso de recebimento de mensagens que contrariem as regras estabelecidas pela GESTORA, nunca as repassar, alertando o responsável da sua área e da Diretora de Compliance e de Gestão de Risco, se for o caso;
- Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail;

XI. BLOQUEIO DE ACESSO A SITES

A Diretora de Compliance e de Gestão de Risco, juntamente com os responsáveis pelo departamento de tecnologia da informação, são responsáveis por monitorar os acessos feitos a sites através de computadores de propriedade da GESTORA, para reporte de eventual mau uso ao Comitê de Compliance, Controles Internos e Ética e bloqueio de acesso a sites proibidos.

São bloqueados sites de jogos de azar, de conteúdo adulto, redes sociais com exceção do Linkedin, plataformas de streaming com exceção do Youtube.

XII. SITES DE ARMAZENAMENTOS DE ARQUIVOS

É permitido o acesso a sites de armazenamento de arquivos em "nuvem".

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores são configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à GESTORA.

Apenas os Colaboradores devidamente autorizados terão acesso às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da GESTORA, mediante segregação física e lógica. Quaisquer exceções deverão ser previamente solicitadas à Diretora de Compliance e de Gestão de Risco, que poderá ou não conceder a exceção.

XIII. GESTÃO DE RISCOS, TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO, CONTINUIDADE DE NEGÓCIO E BACKUPS

Os riscos e incidentes de segurança da informação devem ser reportados à Diretora de Compliance e de Gestão de Risco, que adotará as medidas cabíveis.

O plano de contingência e de continuidade dos principais sistemas e serviços é objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

No caso de divulgação ou acesso indevido de informação, a Diretora de Compliance e de Gestão de Risco deverá ser imediatamente comunicada para a tomada das medidas cabíveis, variando de simples repreensão pelo acesso, ou mensagem ao destinatário errôneo da mensagem enviada para que apague em definitivo o seu conteúdo (se for o caso), até o estudo e implementação efetiva de providências

judiciais, quando e se for o caso, tudo isso sem prejuízo da investigação e eventual punição dos Colaboradores envolvidos, mediante apresentação do caso pela Diretora de Compliance e de Gestão de Risco no Comitê de Compliance, Controles Internos e Ética da GESTORA.

O backup de todos os dados e informações da GESTORA é realizado diariamente na nuvem.

XIV. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

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 crimes cibernéticos são os seguintes:

- *Malware* (vírus, cavalo de troia, *spyware* e *ransomware*);
- Engenharia Social;
- *Pharming*;
- *Phishing scam*;
- *Vishing*;
- *Smishing*;
- Acesso pessoal;
- Ataques de DDoS e botnets;
- 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.

XV. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Uma regra importante de prevenção consiste na segregação de acessos a sistemas e dados que a GESTORA adota, conforme já detalhado nas regras internas que tratam de 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. O acesso ao acervo digital conta com dupla verificação. Quando o Colaborador acessa o office 365 para se identificar por meio de usuário e senha, é enviado um código de segurança no seu celular, garantindo a autenticidade.

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 *antimalware* 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 pela Diretora de Compliance e de Gestão de Risco.

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, CD´s, DVD´s ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na GESTORA.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente.

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 Artigo 25 da Resolução CVM nº 50/2021, 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 caras à prevenção e proteção dos ativos da GESTORA e devem ser observadas integralmente.

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 de TI deve diligenciar para manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

A GESTORA deverá realizar testes de invasão externa, *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica trimestralmente ou sempre que houver mudança significativa em tal estrutura.

Os logs e trilhas de auditoria criados devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

XVI. PLANO DE RESPOSTA

A área de Compliance deve, conjuntamente com o departamento de tecnologia da informação atualizar anualmente 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.

XVII. 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.

XVIII. TESTES DE CONTROLES

A efetividade desta Política é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade da Diretora de Compliance e de Gestão de Risco e reportados ao Comitê de Compliance, Controles Internos e Ética.

Os testes devem verificar se:

- Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;
- Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;
- Há segregação física e lógica;
- Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;
- A manutenção de registros permite a realização de auditorias e inspeções.

XIX. VEDAÇÕES

É vedado ao usuário:

- Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais, sendo proibido, sobretudo, conteúdo pornográfico, racista, subversivo ou ofensivo à moral e aos princípios éticos;

- Divulgar informações ou trocar arquivos com configurações dos equipamentos e de negócios da GESTORA, ou qualquer outra informação sobre a GESTORA, seus negócios, produtos, equipamentos ou Colaboradores, sem prévia aprovação para isso. Em caso de exigência de alguma autoridade ou entidade autorreguladora, solicitar orientação à Diretora de Compliance e de Gestão de Risco;

- Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico;

- Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados residentes na rede da GESTORA;

- Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da GESTORA;

- Alterar qualquer configuração técnica dos softwares que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pela Diretora de Compliance e de Gestão de Risco;

- Contratar provedores de acesso sem autorização prévia da Diretora de Compliance e de Gestão de Risco;

- Redirecionar caixa postal pessoal (e-mail de outros provedores) para a sua caixa postal de correio eletrônico na GESTORA e vice-versa;

XX. PROPRIEDADE INTELECTUAL

Tecnologias, marcas, metodologias e quaisquer informações que pertençam à GESTORA não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

XXI. RASTREAMENTO

É permitido o uso pessoal dos equipamentos de informática e de comunicação de propriedade da GESTORA utilizados pelos Colaboradores para a realização das atividades profissionais. Lembrando que, como tais recursos (e-mails, sistemas, computadores, telefones, *OneDrive* e *SharePoint*; *Windows*, *GS Wave Lite*, etc.) pertencem à GESTORA, estes são rastreáveis e sujeitos a monitoramento, bem como podem se tornar públicos em caso de auditoria, exigência judicial ou regulatória.

XXII. DESCUMPRIMENTO

Na hipótese de divulgação de Informações Confidenciais sem prévia autorização da Diretora de Compliance e/ou descumprimento das diretrizes e vedações expostas, será feita uma análise pelo departamento competente, ficando os Colaboradores envolvidos sujeitos à advertência, suspensão e/ou justa causa, bem como consequências legais cabíveis.

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais mediante prévia autorização da Diretora de Compliance e de Gestão de Risco, em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, seja em âmbito municipal, estadual ou federal, bem como, quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente a Diretora de Compliance e de Gestão de Risco acerca da possibilidade de compartilhamento da Informação Confidencial, a qual deverá se manifestar formalmente sobre o caso.

XXIII. TERMO DE CONHECIMENTO

Os Colaboradores devem aderir formalmente a um termo, comprometendo-se a agir de acordo com esta Política.

Os Colaboradores que tenham acesso a Informações Confidenciais ou participem de processo de decisão de investimento devem solicitar à Diretora de Compliance e de Gestão de Risco eventuais esclarecimentos sobre o tema de segurança de informação e segurança cibernética sempre que houver alguma dúvida.

Anexo I

Termo de Conhecimento da Política de Governança em Privacidade e Segurança da Informação

NOME:		
ÁREA:	**CARGO:**	
DOC. IDENTIDADE Nº	**TIPO:**	**CPF:**

Declaro que tenho conhecimento da Política de Confidencialidade e Segurança da Informação e Segurança Cibernética da GESTORA ("Política"), e que estou ciente do seu teor, o qual está diretamente ligado ao exercício de minhas funções.
De acordo com este termo, comprometo-me a:

a) adotar e cumprir as diretrizes indicadas na Política durante a vigência deste Termo e por prazo indeterminado após sua rescisão;
b) comunicar imediatamente à Diretora de Compliance e de Gestão de Risco qualquer violação desta Política de que eu venha a ter conhecimento, independentemente de qualquer juízo individual, materialidade ou relevância da violação.

Estou ciente e concordo que meus acessos físicos, lógicos, de voz e de imagem podem ser objeto de monitoramento.

Desde já, aceito incondicionalmente atender e cumprir quaisquer novos itens e condições que possam vir a ser considerados partes integrantes desta Política, sem a necessidade de apor assinatura em novo Termo, bem como, em caso de negligência ou imprudência na aplicação desta Política, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

_____, _____ de _____ de 20_____
(local e data)

_____
Assinatura do Colaborador