POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

("Política")

JTR GESTÃO DE RECURSOS LTDA.
("Gestora")

Junho/2026

Sumário

I. INTRODUÇÃO

A informação é um dos principais ativos no mundo dos negócios. Assim, a Gestora estabelece a presente Política de Segurança da Informação e Segurança Cibernética, doravante denominada "Política" ou "PSI", a fim de proteger a informação sob sua responsabilidade de vários tipos de ameaças e garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da organização, dos clientes e do público em geral. Esta Política se aplica aplica-se a todos os sócios, colaboradores ("Colaboradores"), prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Gestora, ou que acesse informações a ela pertencentes.

II. OBJETIVO

Confidencialidade é um princípio fundamental. Aplica-se a quaisquer informações não-públicas referentes aos negócios da Gestora, como também as informações recebidas de seus investidores, contrapartes ou fornecedores, durante o processo natural de condução de negócios. Os Colaboradores não devem transmitir nenhuma informação não-pública a terceiros.

Sob a supervisão do diretor de risco e compliance ("Diretor de Risco e Compliance"), os Colaboradores que forem designados em cada departamento serão responsáveis por implementar e reforçar os procedimentos a fim de proteger a confidencialidade de informações privilegiadas reais ou potenciais. Muitas das atividades destes departamentos são consideradas confidenciais e podem ser usadas somente com aqueles fora do departamento com base na necessidade de conhecimento.

A presente Política de Segurança da Informação e Segurança Cibernética da Gestora, aplica-se a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Gestor, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da Gestora.

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Gestora, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

Em atenção aos dispositivos da Resolução CVM n.º 21/2021 e do Código ANBIMA de Regulação e Melhores Práticas para Administração e Gestão de Recursos de Terceiros, a

Gestora procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Gestora, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

Todos os Colaboradores deverão ler atentamente e entender o disposto nesta Política, bem como deverão firmar o termo de confidencialidade e termo de propriedade intelectual, conforme modelo constante no Anexo I ("Termo de Confidencialidade").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, deve, em qualquer hipótese, ser divulgada fora do ambiente profissional da Gestora, para o desempenho de atividades específicas. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de compliance da Gestora.

Além disso, 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, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Gestora, razão pela qual o Colaborador compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, sendo vedado ao Colaborador, inclusive, apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Gestora, salvo se autorizado expressamente pela Gestora e ressalvado o disposto abaixo.

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

III. REGRAS GERAIS

3.1. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

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

a) *Malware* (vírus, cavalo de troia, *spyware* e *ransomware*);

b) Engenharia Social;

c) *Pharming*;

d) *Phishing* scam;

e) *Vishing*;

f) *Smishing*;

g) Acesso pessoal;

h) Ataques de *DDoS* e *botnets*;

i) Invasões (*advanced persistent threats*).

Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, a Gestora definiu todos os ativos relevantes, fundamentais ao 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.

3.2. CLASSIFICAÇÃO DA INFORMAÇÃO

Para que se possa prevenir eventuais ataques cibernéticos e vazamento de informações, AS informações que transitam pela Gestora são, para fins desta Política, classificadas em 4 (quatro) padrões distintos, a saber:

Informação pública: A informação deve ser classificada como pública quando ela puder ser divulgada a todos, isto é, colaboradores, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio. Apesar de uma informação pública não precisar de nenhum tipo de proteção quanto à questão do sigilo, é conveniente que usuário

nenhum tenha acesso a ela, a menos que precise de tal informação para o desempenho de suas atividades.

Informação interna: A informação deve ser classificada como interna quando não for desejável que ela se torne conhecida por pessoas de fora da Gestora. Contudo, caso haja vazamento e ela se torne de conhecimento público, é característica da informação classificada como interna a impossibilidade da ocorrência de um grande prejuízo à organização. Essas informações não exigem proteções especiais, salvo aquelas entendidas como mínimas para impedir a divulgação externa não intencional.

Informação confidencial: A informação deve ser classificada como confidencial quando sua exposição fora do ambiente da Gestora possa acarretar perdas financeiras, de imagem, de competitividade etc. Para proteção de uma informação confidencial, se faz necessário, além de controles de acesso, controles que garantam sua integridade, pois são informações importantíssimas para as atividades do negócio. Informações confidenciais, por exemplo, jamais podem ser transmitidas via Internet sem o uso de criptografia e, quando descartadas, devem ser tomadas as providências cabíveis para que a informação seja de fato destruída, sem chance de recuperação.

Informação restrita: A informação deve ser classificada como restrita quando acessos não autorizados a ela, mesmo que por membros da própria Gestora, sejam capazes de trazer sérios danos ao negócio. Logo, a informação restrita precisa ser protegida contra acessos internos e externos. São ainda mais importantes que as informações confidenciais e por isso devem receber um grau de proteção ainda mais elevado. Só devem ter acesso a informações restritas pessoas que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado.

3.3. AÇÕES DE PREVENÇÃO

3.3.1. Propriedades dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da Gestora. Não é permitida a utilização de notebooks, tablets ou outros hardwares para operações no âmbito da Gestora, salvo expressa permissão do Diretor de Risco e Compliance.

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

3.3.2. Correio Eletrônico

É proibida a utilização profissional de correio eletrônico particular nas dependências da Gestora ou qualquer outro meio de comunicação privado (whatsapp, messenger, etc.) para enviar informações da Gestora, bem como deve ser evitado o uso deles no ambiente de trabalho.

A Gestora disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais.

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 Gestora.

Se houver necessidade de troca de endereço, a alteração será realizada pela área responsável, mediante autorização e supervisão do Diretor de Risco e Compliance.

O usuário pode acessar o seu correio eletrônico cedido pela Gestora 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 Gestora.

Importante ressaltar que, por se tratar de uma ferramenta de trabalho de propriedade da Gestora, a empresa se reserva ao direito de rastrear, monitorar, gravar e inspecionar, sem aviso prévio, quaisquer informações transmitidas, com o objetivo de evitar riscos decorrentes de ataques externos e do mau uso da ferramenta.

3.3.3. Gravação Telefônica

Em função da natureza das operações realizadas pela Gestora, os ramais estão ligados a sistema de gravação de voz, cujo objetivo é proteger o Colaborador nos eventuais conflitos que surjam nas negociações realizadas pela Gestora e suas contrapartes, bem como possibilita a identificação de situações de não conformidades.

Estas gravações serão armazenadas em nuvem ou qualquer mídia permanente para eventuais consultas posteriores. Periodicamente, serão verificadas pelo Compliance e a escuta por qualquer funcionário só poderá ser realizada com a aprovação desta área e seus Diretores, mediante justificativa acatada pela Diretoria e acompanhada pelo Compliance.

Para atingir esse objetivo, o sistema de monitoramento telefônico contratado pela Gestora grava as chamadas efetuadas ou recebidas nos telefones, permitindo:

- Registrar os números de entrada e saída.
- Monitoração em Real Time de qualquer linha ou ramal.
- Gravar em formato digital todas as ligações recebidas ou realizadas.
- Os arquivos de gravação podem ser extraídos e enviados por e-mail.
- Relatórios Estatísticos.

3.3.4. Uso de Telefones Celulares

Os Colaboradores deverão evitar a utilização de telefones celulares, salvo se utilizado em emergência ou contingência quando houver falha do sistema convencional de telefonia após aprovação da diretoria de compliance ("Diretoria de Compliance"), e para atender ligações pessoais de reconhecida importância. Tal restrição advém de previsão na regulamentação em vigor e garante que todas as comunicações com clientes passam por processo de gravação, seja ela de voz ou de mensagem escrita, para manter o sigilo das informações, conforme inciso I do art. 23. da Resolução CVM nº 21/2021: "O administrador de carteiras de valores mobiliários, pessoa jurídica, deve estabelecer mecanismos para: I – assegurar o controle de informações confidenciais a que tenham acesso seus administradores, empregados e colaboradores".

3.3.5. Estações de Trabalho

Ao se ausentar de sua mesa ou da sala, o Colaborador deverá desligar ou bloquear sua estação de trabalho, para que não haja utilização indevida dos recursos e/ou serviços disponíveis para ele, evitando a exposição de informações a pessoas não autorizadas.

O colaborador não pode apagar arquivos do sistema operacional e de programas aplicativos instalados em sua estação de trabalho, bem como instalar ou remover softwares (programas) e dispositivos móveis, em sua estação de trabalho sem a devida autorização e orientação da área de TI.

Parte dos programas funciona em NUVEM (Cloud Computing) em servidores de terceiros, como PMS, SEARCH (NEOWAY/VADU), HOLMS (GED, além do sistema ZURI (processos – controle de processos de negócios) entre outros, e parte estão dispostos *on premise*, sendo WBA, SUÍTE SYRIUS, E-FINANCEIRA, ECONOMATICA, entre outros.

Diariamente serão realizados backups de todos os arquivos de dados salvos na rede (base de dados, planilhas, textos, etc.). O acesso ao servidor será restrito às pessoas autorizadas.

A instituição tem os cadastros de seus clientes e seus documentos institucionais preservados em arquivo de imagem que ficam fora de sua sede, permitindo utilizá-los ou reconstruí-los de imediato em caso de uma ocorrência que danifique os originais que se encontram na sua sede.

Caso algum computador esteja em manutenção, o funcionário poderá trabalhar com o notebook de backup ou computador de reserva.

3.3.6. Políticas de Senha e Direitos de Acesso

A credencial de acesso a qualquer meio lógico ou físico trata-se de um importante mecanismo de controle e segurança de nossos ativos de informação. As pessoas responsáveis realizarão a revisão dos perfis e dos acessos físicos e lógicos periodicamente ou sempre que necessário, de acordo com o procedimento interno definido para tal e respeitando-se a segregação de funções. As não conformidades eventualmente detectadas durante esses processos poderão ser discutidas pela Diretoria de Compliance e Controle Interno.

3.3.7. Senhas de Acesso

Cada colaborador terá uma senha de acesso e seu uso será pessoal e intransferível que permite o acesso à rede, intranet, internet, softwares ou quaisquer outros dispositivos mantidos pela Gestora. A senha não pode ser compartilhada nem fornecida a terceiros e não deve ser anotada em arquivos físicos ou registradas em meios que permitam sua leitura por terceiros.

As senhas recebidas pelos colaboradores autorizados para acesso aos ambientes e aplicativos devem ser alteradas no primeiro acesso.

Cabe ao colaborador a memorização de suas senhas, sendo sugerida que as mesmas tenham um relativo grau de dificuldade para ser descoberta, mas de fácil memorização.

As senhas de acesso possuem prazos de validade e de alteração determinados de acordo com a criticidade das informações armazenadas e tratadas, como forma de assegurar a confidencialidade ou sempre que identificar que houve tentativa de quebra ou o computador em que usou esteja infectado por vírus.

Caso o colaborador esqueça ou bloqueie sua senha deve solicitar à TI o desbloqueio ou nova senha de acesso.

A Diretoria de Compliance possui uma senha de acesso master que permite monitorar se os colaboradores estão em conformidade com as Políticas e Procedimentos Internos de Controle Interno de Segurança da Informação.

3.3.8. Acesso as Softwares

A Gestora tem uma rede integrada de mais de 30 computadores, revisados quanto à capacidade e nível de atualização de seus componentes trimestralmente, com o suporte técnico da empresa terceirizada contratada, ligados a 3 servidores que armazenam os principais arquivos e processam os "back-up" (em hd externo) e em nuvem. Há um sistema dedicado ao monitoramento e à gravação das telas dos computadores, há um aparelho de hardware para gravação das conversas telefônicas e armazenamento dos arquivos de áudio. Fácil escalabilidade: o número de computadores ligados ao servidor pode ser aumentado com facilidade sem prejudicar a performance.

Quando o colaborador é admitido ou transferido para outra área cabe aos gestores providenciarem junto à TI os acessos necessários e eliminar os acessos desnecessários, garantindo a limitação de acesso às informações críticas, copiando a área de Compliance para monitoramento do novo colaborador e suas atividades.

É possível que por um período pré-determinado o colaborador utilize informações de ambas as áreas em função da necessidade delas. Caso isso seja necessário, o gestor da área originária do colaborador deve solicitar ao Compliance, mediante justificativa, a manutenção dos acessos antigos e a data prevista para manutenção dos mesmos.

3.3.9. Acesso ao Diretório de Rede

Todos os colaboradores possuem um perfil de acesso que possibilitem a realização de suas atividades. Se houver necessidade de novos acessos, deverá solicitar ao Compliance que avaliará junto com o gestor imediato sobre a aprovação ou não do acesso solicitado.

Os perfis de acessos aos diretórios da rede poderão ser sem restrições, só para leitura ou restrição total.

3.3.10. Acesso Remoto

A Gestora disponibiliza, quando necessário, acesso interno à rede e softwares através de conexão remota segura para funcionários devidamente autorizados pela Diretoria de Compliance.

3.3.11. Acesso à Internet

A Gestora disponibiliza os acessos aos sites que os colaboradores necessitam utilizar para realizar e ou facilitar suas tarefas. Caso o colaborador identifique a necessidade de acessar um determinado site que está previamente bloqueado, para fins profissionais, deve solicitar o acesso ao Compliance que, em conjunto com o gestor imediato, aprovará a necessidade ou não do acesso.

Fica proibido o download de arquivos e programas não autorizados ou sem revisão e aprovação da TI. A proibição tem por objetivo evitar que vírus e outros programas indevidos, não licenciados e nocivos apareçam no ambiente de computação da Gestora, com possibilidades de perdas financeiras, de imagem e de confidencialidade das informações.

O eventual uso de e-mail particular para assuntos particulares é tolerado. Não obstante, é terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento à terceiros, bem como com conteúdo político ou outro que possa colocar a Gestora em risco.

3.3.12. Vírus

A qualquer indício de existência de vírus o colaborador deve interromper suas atividades e comunicar imediatamente à TI, por telefone, que executará os procedimentos para a erradicação de vírus no intuito de evitar a propagação do mesmo em todo o ambiente lógico da Gestora.

É terminantemente proibido os esforços individuais e isolados do colaborador para acabar com o vírus, pois podem contribuir para provocar danos ainda maiores, pois, em geral, estes usuários não estão capacitados e/ou não possuem os softwares necessários para erradicação do vírus.

Todos os computadores da Gestora possuem softwares de verificação de integridade (antivírus) com objetivo de proteger os arquivos, softwares e computadores. A desativação do antivírus ou a baixa de softwares de antivírus não homologado pela área de TI sujeita o colaborador a penalidades.

3.3.13. Back-Up e Restauração

O processo de backup nos servidores internos é realizado diariamente para todos os arquivos de dados salvos na rede (base de dados, planilhas, textos, etc.). O acesso ao servidor é restrito às pessoas autorizadas.

Servidores: Cópia de sombra realizada diariamente;

Cópia em disco físico local: realizada às em dois períodos diários (Contempla os dados dos Desktops);

Cópia na Nuvem (Mandic): realizada diariamente (Contempla os dados dos Desktops);

Desktops: Cópia local para o servidor diariamente.

3.3.14. Acesso Físico

A Gestora pela natureza de suas operações, garante a segregação física de suas instalações, com o objetivo de proteger as informações sobre operações, posições e estratégias que só podem ser de conhecimento das áreas responsáveis pelo negócio e seu processamento.

O controle de acesso físico tem por objetivo: impedir acesso não autorizado; identificar e checar permissão de acesso; liberar acesso autorizado; identificar e registrar as tentativas de acessos não autorizados e gerar relatórios sobre a movimentação de acessos ocorridos no local.

A presença de visitantes no interior das instalações deverás sempre ser acompanhada por um colaborador da Gestora.

3.3.15. Acesso ao *Data Center*

Acesso Físico: O controle de acesso ao *Data Center* é feito somente por funcionários autorizados, administradores ou prestadores de serviço acompanhado por tal funcionário.

Acesso Lógico: Todos os computadores possuem acesso limitado ao servidor com níveis de segurança diferenciados e senhas, sendo as senhas eletrônicas renovadas periodicamente para todos os colaboradores e sócios.

3.3.16. *Retirada* de Acesso

Quando um colaborador é desligado da Gestora ou um contrato de prestação de serviços é encerrado, o gestor/contratante deve comunicar, imediatamente, a área de TI para bloquear os acessos físicos e lógicos concedidos.

4. TERMO DE USO E DE POSSE

A Gestora poderá ceder notebook, tablete, modem ou aparelho de telefone celular para o colaborador desenvolver suas atividades profissionais, sendo necessário a assinatura do "Termo de Uso e Posse", onde o colaborador assume toda a responsabilidade pelos mesmos

e pelos softwares nele instalados. Os termos de uso e posse ficarão arquivados na área administrativa.

Quando do desligamento o colaborador deverá devolver todos os equipamentos cedidos para realização de suas atividades profissionais.

5. NOTIFICAÇÃO DE INCIDENTES E ABUSOS

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

Alguns exemplos de incidentes de segurança são:

i) tentativa de uso ou acesso não autorizado a sistemas, ambientes e dados;

ii) tentativa de tornar serviços indisponíveis e modificação em sistemas (sem o conhecimento ou consentimento prévio do TI); e

iii) o desrespeito à PSI da Gestora.

É muito importante que o Colaborador notifique sempre a área de Compliance ao se deparar com uma atitude que considere abusiva ou com um incidente de segurança. As notificações podem ser instrumentos eficazes na mitigação de incidentes e na contenção dos prejuízos, como por exemplo, em casos de fraudes.

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

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política.

Estas providências consistem em:

* Equipe de TI própria ou TI terceirizado (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;

j) Entre outros.

Compliance ou Jurídico Contratado:

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

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

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 pela Área de Compliance, bem como ser formalizado no Relatório de Controles Internos da Gestora.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do código de ética ("Código de Ética") da Gestora.

A Gestora se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus Colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da Gestora e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

6. SUPORTE TÉCNICO

O suporte técnico prestado ao usuário final é realizado através de empresas terceirizadas, responsáveis pelo atendimento de chamados técnicos presencias de hardware, software, telefonia e CFTV, não há limites da chamados e visitas presenciais. Visitas periódicas a cada 15 dias, visitas extras realizadas conforme o prévio agendamento incluindo horário não comercial e finais de semana.

7. PLANOS DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Os procedimentos para acessos físicos e lógicos nas situações de emergências e contingências estão descritos no Plano de Continuidade de Negócios, no qual estão abrangidos os procedimentos a serem adotados nestas circunstâncias de forma a que todos os colaboradores estejam aptos a exercer suas atividades, sem descontinuidade.

8. DECLARAÇÃO DE RESPONSABILIDADE E MEDIDAS DISCIPLINARES

Os colaboradores devem aderir formalmente ao Termo de Confidencialidade, e o Termo de Ciência da Política Corporativa de Segurança da Informação, comprometendo-se a agir de acordo com as PSI e demais normativos da Gestora e de seus reguladores e autorreguladores.

As violações à PSI e demais normativos estão sujeitas às sanções disciplinares previstas no Código de Ética Corporativo da Gestora.

9. DISPOSIÇÕES GERAIS (Revisão da Política e Histórico)

Neste documento, a Gestora detalha os principais pontos de sua Política Corporativa de Segurança da Informação e Cibersegurança que irão vigorar durante o ano calendário. Esta política será submetida à revisão anual ou em períodos inferiores a este, sempre que necessário.

Todos os Colaboradores recebem uma cópia desta política e todos têm o dever de conhecer e aplicar as regras e procedimentos aqui estabelecidos. Qualquer dúvida deverá ser esclarecida com a Diretoria de Compliance.

Versão	Data	Modificações
01	Junho/2026	Original

ANEXO I

TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o nº _____, doravante denominado Colaborador, e **JTR GESTÃO DE RECURSOS LTDA.**, inscrita no CNPJ sob o nº 51.921.562/0001-09 ("Gestora").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, seus sócios e clientes, aqui também contemplados os próprios fundos, incluindo:

a) Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Gestora;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Gestora;
d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;
e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
g) Outras informações obtidas junto a sócios, diretores, funcionários, trainees ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores,

clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1. O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Gestora, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "Insider Trading", "Dicas" e "Front Running", seja atuando em benefício próprio, da Gestora ou de terceiros.

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

3.2. O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da

Gestora e de seus sócios, razão pela qual 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, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder; e

(iii) Nos termos da Lei nº 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

5.2. A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Tenho ciência dos direitos, obrigações e penalidades aplicáveis constantes da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - "LGPD") e me comprometo a adotar todas as medidas necessárias para utilização dos dados e informações aos quais tiver acesso em decorrência das atividades desempenhadas em conformidade com o estabelecido pela LGPD e com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Gestora.

6.1. Estou ciente, ainda, de meu compromisso de comunicar ao Encarregado[1], conforme definido pela Gestora, qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Gestora.

6.2. Na qualidade de pessoa física titular de Dados Pessoais ("Titular de Dados Pessoais"), estou ciente e de acordo que a Gestora, na qualidade de "Controladora" para fins de atendimento às disposições da LGPD, tome decisões relativas ao Tratamento de meus Dados Pessoais[2], incluindo operações como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração ("Tratamento") durante todo o período em que eles forem pertinentes, observados os princípios e as garantias ora estabelecidas pela referida lei.

6.3. Também na qualidade de Titular de Dados Pessoais, estou ciente de que, a qualquer tempo, mediante requisição à Controladora, tenho o direito de (i) confirmar a existência de Tratamento e acessar meus Dados Pessoais, (ii) corrigir dados incompletos, inexatos ou desatualizados, (iii) solicitar a anonimização, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD, (iv) solicitar a portabilidade de meus Dados Pessoais a outro fornecedor de serviço, (v) solicitar a eliminação dos Dados

[1] "Encarregado" é a pessoa indicada pela Gestora para atuar como canal de comunicação entre os Titulares dos Dados Pessoais e a Autoridade Nacional de Proteção de Dados.
[2] Para os fins do presente Termo de Compromisso são considerados Dados Pessoais toda informação relacionada a uma pessoa física que a torne diretamente identificada ou identificável.

Pessoais tratados com o meu consentimento, (vi) solicitar informações sobre o compartilhamento dos meus dados pela Controladora e sobre a possibilidade de não fornecer o consentimento e as consequências dessa negativa, e (vii) me opor ao Tratamento de meus Dados Pessoais em caso de descumprimento da LGPD.

6.4. Reconheço que a Controladora poderá compartilhar os Dados Pessoais com outros agentes de Tratamento de dados, tais como escritórios de contabilidade, agências de turismo, planos de saúde e instituições financeiras, caso seja necessário, bem como que poderá compartilhar em seu website os Dados Pessoais, incluindo minha identificação como Colaborador da Gestora e meu histórico profissional, observados os princípios e as garantias ora estabelecidas pela LGPD, com o que, desde já, estou de acordo.

6.5. Estou ciente de que a Controladora poderá manter armazenados os Dados Pessoais necessários após o término da relação contratual, por prazo determinado em lei, para fins de cumprimento de obrigações legais e/ou regulatórias, bem como para exercer seus direitos em processos administrativos e/ou judiciais.

6.6. Comprometo-me, enfim, a observar em tudo às instruções fornecidas pela Gestora, na qualidade de Controladora, acerca do Tratamento que deverá ser concedido aos Dados Pessoais aos quais tiver acesso em razão de minhas atividades, bem como a sempre agir de acordo com as disposições da LGPD e das normas internas da Gestora quanto à privacidade e proteção de Dados Pessoais.

7. Este Termo é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

8. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[Cidade], [---] de [---] de [---].

_____

[COLABORADOR]

_____

JTR GESTÃO DE RECURSOS LTDA.

Testemunhas:[3]

1.	2.
Nome:	Nome:
CPF/MF:	CPF/MF:

[3] A Lei nº 14.620/2023 passou a conferir força executiva aos documentos constituídos ou atestados por meio eletrônico, que tenham sido assinados mediante o uso de qualquer modalidade de assinatura eletrônica prevista em lei, dispensando as assinaturas de testemunhas nos casos em que a integridade das assinaturas apostas pelas partes for conferida pelo provedor de assinatura (i.e. tal como já como ocorre quando há a assinatura com certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.)

ANEXO II

TERMO DE PROPRIEDADE INTELECTUAL

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

(i) que a disponibilização pelo Colaborador à **JTR GESTÃO DE RECURSOS LTDA**., inscrita no CNPJ sob o nº 51.921.562/0001-09 ("Gestora"), nesta data, dos documentos contidos no pen drive da marca [•], número de série [•] ("Documentos"), bem como sua futura utilização pela Gestora, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;

(ii) ciência e concordância de que quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, nos Documentos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gestora, exceto se aprovado expressamente pela Gestora.

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

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

[Cidade], [---] de [---] de [---].

_____

[COLABORADOR]

APÊNDICE - LISTA DOS ARQUIVOS GRAVADOS NOS PEN DRIVES