

MANUAL DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. O presente manual, aprovado em 29 de novembro de 2017, dispõe acerca da política de segurança da informação (“**Política**”) da **3J Gestora de Recursos Ltda.** (“**Sociedade**”), tendo como objetivo estabelecer regras que orientem o controle de acesso a informações confidenciais pelos diretores, empregados e prestadores de serviços (“**Colaborador**” ou, em conjunto, “**Colaboradores**”) da Sociedade, inclusive através do estabelecimento de regras para a utilização de equipamentos e e-mails da Sociedade, para gravação de cópias de arquivos, para *download* e instalação de programas nos computadores da Sociedade dentre outras.

Versão	3.0
Aprovada em	29/11/2017
Aprovada por	Diretor de Compliance
Revisão anterior	12/05/2023
Última revisão	18/09/2026
Próxima revisão	até 30/09/2027
Natureza da revisão	Revisão de conteúdo. Inclusão de autenticação multifator, uso de equipamentos pessoais e trabalho remoto, e contratação de serviços em nuvem; atualização da rotina de backup para periodicidade diária com ambiente de contingência; inclusão do dever de comunicação de incidente com dados pessoais; articulação expressa com a Política de Privacidade e Proteção de Dados; instituição de quadro de controle de versão.

2. Nesse sentido, todos os Colaboradores da Sociedade firmarão o Termo de Adesão anexo ao presente manual (Anexo I), tomando conhecimento e expressamente anuindo com o quanto segue:

(i) Os arquivos físicos com os dados e informações relativas a cada uma das atividades desenvolvidas pela Sociedade ficarão alocados no respectivo espaço físico de cada uma das áreas. Desta forma, somente os Colaboradores, cujas atividades forem relacionadas com o mercado financeiro e de capitais, terão acesso a informações confidenciais e sigilosas relativas à sua atividade.

(ii) Os equipamentos e computadores disponibilizados aos Colaboradores da Sociedade deverão ser utilizados com a finalidade de atender aos interesses comerciais da Sociedade, sendo permitida a sua utilização para fins particulares de forma moderada.

(iii) A gravação de cópias de arquivos e instalação de programas em computadores da Sociedade deverá respeitar as regras estabelecidas no Manual de Política de Sigilo e Confidencialidade, bem como os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

(iv) *Downloads* de qualquer natureza podem ser realizados, desde que de forma ponderada, respeitando o espaço individual de cada usuário. Periodicamente, a critério do Comitê de

Compliance, poderão serão realizadas inspeções nos computadores para averiguação de *downloads* impróprios, não autorizados ou gravados em locais indevidos.

(v) O correio eletrônico disponibilizado pela Sociedade ("**E-mails Corporativos**") caracteriza-se como correio eletrônico corporativo para todos os efeitos legais, especialmente os relacionados aos direitos trabalhistas, sendo sua utilização preferencial voltada para alcançar os fins comerciais aos quais se destina. É permitida a utilização pessoal de forma moderada.

(vi) As mensagens enviadas ou recebidas por meio de E-mails Corporativos, seus respectivos anexos e a navegação por meio da rede mundial de computadores por meio de equipamentos da Sociedade ou dentro das instalações da Sociedade poderão ser monitoradas.

(vii) Os E-mails Corporativos recebidos pelos Colaboradores da Sociedade, quando abertos, deverão ter seu conteúdo verificado pelo Colaborador, não sendo admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem. Os arquivos de E-mails Corporativos poderão ser inspecionados pela Sociedade, a critério do Comitê de Compliance, a qualquer tempo e independentemente de prévia notificação.

(viii) Todos os programas de computador utilizados pelos Colaboradores da Sociedade devem ter sido previamente autorizados pelo responsável pela área de informática da Sociedade. Os computadores podem ser inspecionados pela Sociedade a qualquer tempo para a verificação da observância do disposto na presente Política. É terminantemente proibido o uso de programas ilegais (PIRATAS). Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da empresa.

(ix) Cada um dos Colaboradores da Sociedade, no momento de sua contratação, receberá uma senha secreta, pessoal e intransferível para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo da Sociedade.

(x) O acesso a informações confidenciais e sigilosas será restrito e poderá ser diferenciado conforme os níveis hierárquicos e as funções desempenhadas pelos Colaboradores da Sociedade a critério do Comitê de Compliance. O controle de acesso a tais informações será realizado por meio das senhas pessoais dos Colaboradores, que, a critério do Comitê de Compliance, poderão respeitar uma ordem de graduação com diferentes níveis de acessibilidade a arquivos, pastas e diretórios da rede corporativa.

(xi) Cada Colaborador terá acesso a pastas eletrônicas diretamente relacionadas às atividades desenvolvidas pela sua área. Apenas o administrador do sistema, o prestador de serviços de tecnologia e os diretores da Sociedade terão acesso a todas as pastas. Serão criados dentro de nossa rede de computadores diretórios exclusivos para cada área, sendo esses diretórios bloqueados para as áreas que não sejam diretamente ligadas às informações contidas nos mesmos.

(xii) O acesso aos sistemas corporativos que suportem informação confidencial ou restrita, em especial ao sistema interno de gestão patrimonial, exige autenticação

multifator. É vedado ao Colaborador desativá-la, contorná-la ou compartilhar os respectivos códigos de verificação. O bloqueio automático da conta após tentativas sucessivas de acesso inválido constitui medida de proteção e não deve ser tratado como falha do sistema. O Colaborador deverá bloquear a tela sempre que se ausentar da estação de trabalho.

(xiii) A utilização de equipamentos pessoais no desempenho de atividades da Sociedade somente é admitida mediante autorização prévia do setor de Compliance, e sujeita-se às mesmas regras aplicáveis aos equipamentos corporativos, incluindo a manutenção de sistema operacional e antivírus atualizados e a vedação à instalação de programas não homologados. Em regime de trabalho remoto, é vedado o acesso a informação confidencial ou restrita por meio de redes públicas ou compartilhadas sem canal cifrado.

(xiv) A contratação e o uso de serviços de computação em nuvem para armazenamento ou processamento de informação da Sociedade dependem de aprovação prévia do setor de Compliance, que avaliará a criticidade do serviço, o acesso a dados pessoais, a jurisdição do provedor e sua situação regulatória, na forma da Política de Seleção e Contratação de Terceiros. É vedado ao Colaborador transferir informação confidencial ou restrita para serviços de armazenamento pessoal ou contas não corporativas.

3. Em complementação aos procedimentos acima, que deverão ser observados por todos os Colaboradores, a Sociedade instalará *firewall* de segurança nos servidores para acesso à sua rede, visando manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus será atualizado diariamente. O *back up* de arquivos será realizado de forma sistemática com unidade de disco externa ao servidor e os *links* são dedicados e seguros, via rádio.

4. Adicionalmente, o backup de arquivos é realizado diariamente, de forma automatizada e verificada, com armazenamento em local seguro. A Sociedade mantém, ainda, ambiente de contingência apto a sustentar a operação em caso de indisponibilidade do ambiente primário, cuja eficácia é objeto de teste periódico documentado. Novas tecnologias de solução de backup serão estudadas para futuras implementações, conforme necessidade da Sociedade e orientação do Comitê de Compliance, ouvidos os técnicos de informática e o setor responsável. Por meio de software de monitoramento remoto seguro, o prestador de serviços de tecnologia poderá otimizar o controle sobre a rede.

5. É de responsabilidade do Gestor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios abaixo:

- Pública: Toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.
- Interna: Toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
- Confidencial: Toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode

causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

- Restrita: Toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Os gestores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

Todos na empresa não devem deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório ou mídia confidencial ou restrita sobre suas mesas.

6. Cabe ao setor de Compliance da Sociedade, atuando sob a orientação e em conjunto com o Comitê de Compliance da Sociedade e seus membros, a fiscalização e verificação do cumprimento do disposto nesta Política, conforme regras e mecanismos estabelecidos no Manual de Compliance da Sociedade.

6. O setor e Comitê de Compliance visará promover a aplicação da presente Política, bem como o controle, a supervisão e a aprovação de exceções em relação à presente Política, sendo responsabilidade do Comitê de Compliance assegurar a implementação de mecanismos eficientes capazes de resguardar a segurança das informações de propriedade da Sociedade ou de terceiros em relação às quais a Sociedade tenha tido acesso, bem como a identificação de quaisquer infrações às regras aprovadas na forma da presente Política.

7. O Comitê de Compliance exercerá suas atribuições de acordo com o disposto no Manual de Compliance, cabendo a este e/ou a qualquer de seus membros: (i) avaliar os procedimentos e processos utilizados para assegurar o cumprimento do disposto na presente Política; (ii) avaliar eventos de potencial descumprimento das normas desta Política por Colaboradores e definir os procedimentos a serem adotados para a sua repressão e/ou aplicar penalidades ou promover mecanismos para a reparação de danos sofridos pela Sociedade ou terceiros em função do descumprimento da Política ora estabelecida; e (iii) propor alterações e ajustes à presente Política.

8. É proibido aos usuários da rede:

- Acessar, copiar ou armazenar programas de computador ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais, bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, homofóbico, racista, de apologia a crimes, dentre outros;
- Passar-se por outra pessoa ou esconder, por qualquer meio, a própria identidade quando utilizar os recursos computacionais ou quaisquer outros de propriedade da

GESTORA, colocados à disposição do colaborador em razão do exercício de sua função;

- Usar ou divulgar informações confidenciais obtidas para benefícios pessoais (oportunidades de emprego, investimentos, dentre outros) mesmo após o término de seu vínculo com a GESTORA;
 - Alterar os sistemas padrões, sem autorização;
 - Divulgar quaisquer informações confidenciais para concorrentes e/ou qualquer pessoa não ligada às atividades da Empresa;
 - Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes à Empresa;
 - Violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas, sistemas de alarme e demais mecanismos de segurança e restrição de acesso;
 - Utilizar acesso através de modem, ou qualquer outra forma de conexão não autorizada, quando conectado às redes instaladas nas dependências da 3J;
9. Em caso de ocorrência de vazamento de informações ou incidente de segurança, o Colaborador deve registrar e comunicar o fato imediatamente à área de Compliance ou a membro do Comitê de Segurança das Informações. Quando o incidente envolver dados pessoais, a área de Compliance acionará o Encarregado de Proteção de Dados, a quem competirá avaliar o risco aos titulares e adotar as providências de comunicação à Autoridade Nacional de Proteção de Dados e aos titulares afetados, na forma da Lei nº 13.709/2018 e da Política de Privacidade e Proteção de Dados da Sociedade.
- Criar blogs ou comunidades na Internet, ou qualquer ambiente virtual semelhante, fazendo uso, sem autorização expressa, da logomarca ou do nome 3J;

9. Em caso de ocorrência de um vazamento de informações ou incidente de segurança, o colaborador deve registrar e comunicar o fato imediatamente à área de Compliance ou a algum membro do Comitê de Segurança das Informações.

11. Este Manual disciplina a conduta dos Colaboradores no trato da informação da Sociedade e deve ser lido em conjunto com a Política de Privacidade e Proteção de Dados, que rege o tratamento de dados pessoais e os direitos dos respectivos titulares. Em caso de aparente conflito entre os dois documentos quanto a dados pessoais, prevalece a Política de Privacidade e Proteção de Dados. Este Manual será revisado anualmente, ou sempre que houver alteração legislativa, mudança relevante no ambiente tecnológico da Sociedade ou ocorrência de incidente que recomende sua reavaliação.

10. O não cumprimento desta Política de Segurança da Informação implica falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

12 de Maio de 2023

* * *

ANEXO I

TERMO DE ADESÃO

Eu, _____, portador da Cédula de Identidade nº _____, inscrito no CPF/MF sob o nº _____, declaro para os devidos fins que:

1. Tenho total conhecimento da existência do Manual de Política de Segurança da Informação da **3J Gestora de Recursos Ltda.** (“**Sociedade**”), aprovado em 29 de novembro de 2017, o qual recebi e li, sendo que comprometo-me a observar integralmente seus termos e condições.
2. Sei, a partir desta data, que a não observância dos termos do Manual de Política de Segurança da Informação da Sociedade poderá implicar na caracterização de falta grave, fato que poderá ser passível da aplicação das penalidades cabíveis, inclusive demissão por justa causa.
3. Ademais, estou ciente que, caso haja o vazamento de informação confidencial advindo da utilização de minha senha pessoal, poderei ser responsabilizado tanto civil, quanto penalmente.
4. As regras estabelecidas no Manual de Política de Segurança da Informação da Sociedade não invalidam nenhuma disposição relativa a qualquer norma interna estabelecida pela Sociedade, mas apenas servem de complemento e esclarecem como lidar com determinadas situações na execução de minhas atividades profissionais.

São Paulo, _____ de 20____.
