PROGRAMA DE SEGURANÇA CIBERNÉTICA
BPJ CAPITAL GESTÃO DE RECURSOS LTDA.

SETEMBRO DE 2020

SUMÁRIO

1. OBJETIVO

Este *"Programa de Segurança Cibernética"* ("Programa") da BPJ Capital Gestão de Recursos Ltda. ("BPJ" ou "Gestora"), têm por objetivo garantir a disponibilidade das atividades desenvolvidas pela Gestora, buscando, prioritariamente a proteção as informações confidenciais sob a posse desta, dos veículos de investimentos sob sua gestão e dos seus investidores.

Este Programa foi elaborado em conformidade com a Instrução da Comissão de Valores Mobiliários ("CVM") nº 558, de 26 de março de 2015, conforme alterada ("Instrução CVM 558"), o "*Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA") de Regulação e Melhores Práticas para Administração de Recursos de Terceiros"* ("Código ART") e o Guia de Cibersegurança ANBIMA e é aplicado a todos os funcionários, estagiários, sócios, administradores e prestadores de serviços terceirizados da Gestora (quando em conjunto, "Colaboradores").

Este Programa deve ser lido em conjunto com as demais políticas, códigos e manuais da BPJ, os principais normativos emitidos pela CVM, os Códigos ANBIMA e demais legislações aplicáves.

Para os fins deste Programa, informações confidenciais são as informações da Gestora, dos veículos de investimentos sob sua gestão, dos investidores, informações que ainda não sejam de domínio público ou que a BPJ não deseje que sejam divulgadas.

Dessa forma, é terminantemente proibida a divulgação de informações confidenciais para fora dos escritórios da Gestora ou para pessoas, mesmo que dentro ou fora da BPJ, não necessitem ou não devam ter acesso a tais informações.

Qualquer informação confidencial somente poderá ser fornecida ao público em geral, por qualquer meio, caso tenha sido previamente autorizado pelo Departamento de *Compliance*.

Todas as informações processadas e armazenadas pela Gestora devem ser armazenadas em ambiente seguro e protegidas de terceiros não autorizados.

Ressaltamos que o suporte de tecnologia da informação da Gestora é terceirizado, realizado por empresa prestadora de serviços de tecnologia da informação, de modo que, não temos nenhum colaborador interno do setor ("Auxiliares de TI").

Os sistemas de informação, a infraestrutura tecnológica, os documentos e as informações internas são considerados ativos da Gestora, e as medidas de prevenção e manutenção descritas neste Programa visam assegurar a: (i) confidencialidade, (ii) integridade, e (iii) disponibilidade dos dados e dos sistemas utilizados, sejam eles da Gestora ou dos seus investidores, conforme definição abaixo:

a) **Confidencialidade:** garantir que as informações tratadas pela BPJ sejam disponibilizadas somente a um grupo de pessoas autorizadas, impedindo a exposição de dados restritos e acessos não autorizados;

b) **Integridade:** garantir a integridade das informações, de forma que elas sejam íntegras e sem alterações feitas por pessoas não autorizadas;

c) **Disponibilidade:** garantir a disponibilidade de informações aos usuários autorizados sempre que necessário.

2. IDENTIFICAÇÃO DOS ATIVOS RELEVANTES

No âmbito das atividades da BPJ, foram identificados uma lista de ativos relevantes e a proteção de tais ativos requer maior atenção e proteção:

a) **Informações Confidenciais:** informações dos investidores, Colaboradores, da Gestora e dos veículos sob sua gestão,

b) ***Softwares* e planilhas:** *softwares* e planilhas utilizados pela BPJ para execução das suas atividades de negócio;

c) **Arquivos com evidências dos monitoramentos, processos e controles:** informações geradas por meio dos processos de controles internos do Departamento de Risco, do Departamento *de Compliance* e do Departamento de Gestão de Recursos em conjunto com os Auxiliares de TI.

Em relação aos riscos relacionados à segurança cibernética, a BPJ verificou, nos termos do Guia de Cibersegurança ANBIMA, as seguintes principais ameaças para os seus negócios:

a) **Invasões externas:** ataques cibernéticos, normalmente realizados por *hackers*, que utilizam meios para explorar fragilidades e deficiências específicas do ambiente tecnológico, podendo causar a interrupção temporária e/ou a continuidade dos seus negócios;

b) **Engenharia social:** método que manipula o conhecimento dos usuários da instituição para obter principalmente informações confidenciais da Gestora

c) ***Malwares*:** softwares desenvolvidos para corromper a segurança da rede de computadores como virus, *ransomware, spyware, phishing*, etc.

A lista indicada acima não pretende ser exaustiva e serve para exemplificar os principais fatores de risco que a BPJ pode estar exposta no curso normal das suas atividades.

Estes riscos serão constantemente acompanhados pelo Departamento de *Compliance*, baseados nas orientações de segurança fornecidas pelos Auxiliares de TI.

3. AÇÕES DE PROTEÇÃO E PREVENÇÃO

Visando mitigar os riscos identificados, a BPJ adotará de forma contínua as medidas indicadas abaixo para proteger as informações confidencias e a disponibilidade das suas atividades:

3.1. Regra geral de conduta

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponibilizados nos escritórios da BPJ sem a prévia autorização do Departamento de *Compliance*,

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem destinados a execução e/ou desenvolvimento dos negócios da BPJ.

Nestes casos, o Colaborador que estiver em posse dos referidos arquivos será o responsável direto por sua boa conservação, integridade e manutenção da sua confidencialidade.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação.

O descarte de documentos físicos, que contenham informações confidenciais, deverá ser realizado imediatamente após seu uso de maneira a evitar sua recuperação, sendo recomendável o seu descarte total.

3.2. Uso dos sistemas internos da Gestora

Os Colaboradores devem se abster de utilizar pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva do desempenho de sua atividade na BPJ.

É proibida a conexão de equipamentos na rede da BPJ que não estejam previamente autorizados, novos equipamentos e/ou sistemas deverão ter suas configurações realizadas pelos Auxiliares de TI.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

Será obrigatória a alteração de senha de acesso aos equipamentos (*login* de usuário), conforme orientação dos Auxiliares de TI, utilizando modelo de definição de senha de difícil identificação por parte de potenciais "*hackers*" externos.

O acesso a *sites* e *blogs*, bem como o envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, como também o envio ou repasse de *e-mails* com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da BPJ.

Programas instalados nos computadores, especialmente feitos *downloads* da internet, sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia, além de avaliação de segurança pelos Auxiliares de TI.

Não é permitida a instalação de softwares ilegais ou que possuam seus direitos autorais protegidos sem prévia autorização do Departamento de *Compliance*.

Todo conteúdo armazenado na rede da BPJ, inclusive arquivos pessoais e *e-mails*, serão passíveis de monitoramento.

A confidencialidade dessas informações será respeitada, e seu conteúdo será disponibilizado ou divulgado somente ao Departamento de *Compliance* para efeito de monitoramento e cumprimento das regulação e políticas internas.

3.3. *Firewal* e *softwares* antivírus

A BPJ utilizará serviços de proteção projetados para detectar e bloquear acessos não autorizadas em sua rede interna, como por exemplo, *malwares* e tentativas de invasão por vírus.

Os dispositivos de antivírus são projetados para detectar, evitar e quando possível excluir programas que possam afetar os sistemas da BPJ.

As informações internas da BPJ também serão armazenadas em *cloud* para efeito de *backup*, em caso de indisponibilidades dessas informações, os procedimentos descritos na *"Política de Continuidade de Negócios"*, poderão ser acionados sob a orientação do Departamento de *Compliance*.

4. MECANISMOS DE SUPERVISÃO

Os Auxiliares de TI serão responsáveis por monitorar a segurança cibernética da Gestora e serão supervisionados pelo Departamento de *Compliance*, os quais, em conjunto realizarão a análise dos relatórios periódicos de contendo informações de vulnerabilidades e sugestões de melhorias, a fim garantir a disponibilidade das atividades da Gestora.

5. PLANO DE RESPOSTA

A definição de um plano de resposta efetivo é vital para proteger as atividades da BPJ.

Os recursos tecnológicos disponibilizados pela Gestora serão monitorados por *software* que fornecerá, de forma automática, informações atualizadas sobre as tentativas de invasão e a possível indisponibilidade de algum serviço.

Por meio da análise das informações fornecidas em relatórios, a gestora poderá verificar a necessidade ou não da tomada de alguma providência.

Os Colaboradores que identificarem situações de risco iminente, deverão informar imediatamente aos Auxiliares de TI ou ao Departamento de *Compliance*, para que seja iniciado o procedimento de avaliação de um suposto ataque cibernético.

Após análise da situação, os Auxiliares de TI darão orientações ao Departamento de *Compliance* sobre forma de conduzir suas atividades da forma mais segura naquele momento.

6. REVISÃO DO PROGRAMA

Considerando a rápida evolução das práticas e soluções sobre cibersegurança, exigindo constantes adaptações, este programa será revisado e, se necessário, atualizada pelo Departamento de *Compliance*, a cada 24 (vinte e quatro) meses, ou quando houver alteração na regulamentação que demande novas modificações.

Durante a revisão, será avaliada a eficácia da implantação durante a sua vigência, a identificação de novos riscos, bem como avaliação de riscos residuais desde a sua implementação.