BLP GESTORA DE RECURSOS LTDA.

Política de Segurança Cibernética

Janeiro 2020

I. OBJETIVO

A Política de Segurança Cibernética ("Política") da BLP Gestora de Recursos Ltda. ("BLP" ou "Gestora"), têm por objetivo garantir a disponibilidade das atividades desenvolvidas pela BLP, buscando, prioritariamente a proteção as informações confidenciais sob a posse da BLP, dos veículos de investimentos sob sua gestão e dos seus investidores.

Para os fins desta Política, informações confidênciais 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 BLP não deseje que sejam divulgadas.

Dessa forma, é terminantemente proibida a divulgação de informações confidênciais para fora dos escritórios da Gestora ou para pessoas, mesmo que dentro ou fora da BLP, 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 pela Diretoria.

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

Os sistemas de informação, a infra-estrutura tecnológica, os documentos e as informações internas são considerados ativos da companhia, e as medidas de prevenção e manutenção descritas na Política 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:

i. **CONFIDENCIALIDADE:** garantir que as informações tratadas pela BLP sejam disponibilizadas somente a um grupo de pessoas autorizadas, impedindo a exposição de dados restritos e acessos nao autorizados;

ii. **INTEGRIDADE:** garantir a integridade das informações, de forma que elas sejam íntegras e sem alterações feitas por pessoas não autorizadas;

iii. **DISPONIBILIDADE:** garantir a disponibilidade de informações aos usuários autorizados sempre que necessário.

II. IDENTIFICAÇÃO DOS ATIVOS RELEVANTES

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

- **Informações Confidenciais:** informações dos investidores, colaboradores, da gestora e dos veículos sob sua gestão,

- **Softwares e planilhas:** softwares e planilhas utilizados pela BLP para execução das suas atividades de negócio;

- **Arquivos com evidências dos monitoramentos, processos e controles:** informações geradas por meio dos processos de controles internos das áreas de Risco, Compliance, Gestão e TI.

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

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

- **Engenharia social:** método que manipula o conhecimento dos usuários da instituição para obter principalmente informações confidênciais da companhia;

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

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

Estes riscos serão constantemente acompanhados pelas equipes de Risco e Compliance, baseados nas orientações de segurança fornecidas pela equipe de TI contratada pela Gestora.

I. AÇÕES DE PROTEÇÃO E PREVENÇÃO

Visando mitigar os riscos identificados a BLP adotará de forma contínua as seguintes medidas para proteger as informações confidencias e a disponibilidade das suas atividades:

a. **Regra geral de conduta**

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponibilizados nos escritórios da BLP sem a prévia autorização da Diretoria,

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 BLP. 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.

b. 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 BLP.

É proibida a conexão de equipamentos na rede da BLP que não estejam previamente autorizados, novos equipamentos e/ou sistemas deverão ter suas configurações realizadas pela equipe 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 da equipe de T.I., 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 BLP.

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 pela equipe de TI.

Não é permitida a instalação de softwares ilegais ou que possuam seus direitos autorais protegidos sem prévia autorização da Diretoria.

Todo conteúdo armazenado na rede da BLP, inclusive arquivos pessoais e e-mails, serão passíveis de monitoramento. A confidencialidade dessas informações será respeitada, e seu conteúdo será disponibilizado ou divulgado somente a equipe de Risco e Compliance para efeito de monitoramento e cumprimento das regulação e políticas internas.

c. Firewal e softwares antivírus

A BLP 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 virus.

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

As informações internas da BLP também serão armazenadas em *cloud* para efeito de *backup*, em caso de indisponibilidades dessas informações, os procedimentos descritos na Política de Continuidade de Negócios, pederão ser acionados sob a orientação da Diretoria.

I. MECANISMOS DE SUPERVISÃO

A empresa prestadora de serviços de TI será responsável por monitorar a segurança cibernética da Gestora e contará com sob a supervisão das áreas de Risco e Compliance e juntas realizarão a análise dos relatórios periódicos de contendo informações de vulnerabilidades e sugestões de melhorias,a fim garantir a disponibilidade das atividades da companhia.

II. PLANO DE RESPOSTA

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

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 a equipe de TI, para que a mesma inicie os procedimentos de avaliação de um suposto ataque cibernético.

Após análise da situação, a equipe de TI dará orientações à Diretoria sobre forma de conduzir suas atividades da forma mais segura naquele momento.

III. REVISÃO DA POLÍTICA

Considerando a rápida evolução das práticas e soluções sobre cibersegurança, exigindo constantes adaptações, esta política será revisada e, se necessário, atualizada pelo Compliance, a cada 24 (vinte e quatro) meses, ou quando houver alteração na Regulação 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.