INVESTPORT GESTÃO E CONSULTORIA DE INVESTIMENTOS LTDA.

MANUAL DE SEGURANÇA CIBERNÉTICA

JUNHO/2019

1. Introdução

1.1 Objetivo

Este Manual de Segurança Cibernética ("Manual") tem por objetivo estabelecer as regras, procedimentos e controles de segurança cibernética da **INVESTPORT GESTÃO E CONSULTORIA DE INVESTIMENTOS LTDA.** ("INVESTPORT"), com o objetivo de proteger as informações sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme estipulado pelo Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, seguindo as recomendações e diretrizes do Guia de Cibersegurança da ANBIMA, datado de dezembro de 2017.

1.2 Aplicabilidade do Manual

Este Manual aplica-se a todos os Colaboradores que, por meio de suas funções na INVESTPORT, poderão ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

Todos os Colaboradores devem se assegurar do perfeito entendimento do completo conteúdo deste Manual, bem como das leis e normas aplicáveis à INVESTPORT.

2. Comitê de Segurança Cibernética

O Comitê de Segurança Cibernética será composto pelo Diretor de Compliance, Sr. Felipe Arnold Schmidt e a equipe de TI terceirizada da INVESTPORT. O Comitê se reunirá semestralmente, ou quando necessário.

3. Procedimentos de Segurança Cibernética

Segundo as recomendações da ANBIMA, cabe a INVESTPORT (i) identificar os riscos, (ii) atuar na prevenção, (iii) monitorar, (iv) executar plano de resposta e (v) manter treinamento e reciclagem.

(i) Identificação e Avaliação de Riscos (*Risk Assessment*):

A INVESTPORT deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta, como:

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

(ii) Prevenção e Proteção:

A INVESTPORT possui regras para controlar o acesso, com regras para concessão de senhas de acesso aos diferentes dispositivos, sistemas e rede. Os colaboradores possuem acesso à rede e senha primaria da empresa, enquanto convidados acessam uma rede paralela de *wi-fi*, com duração determinada.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto aos arquivos e sistemas internos ou na nuvem são inventariados por empresa de TI.

Todo equipamento novo passa por testes e homologações antes da entrada na rede primaria da INVESTPORT.

A INVESTPORT realiza backup de todos os seus arquivos e sistemas, com rotinas pré-determinadas no Manual de ética, Compliance e Regulatório, retratado no Anexo I ao presente Manual.

A INVESTPORT conta com antivírus e *firewalls* em todas estações de trabalho, servidores e redes. Não é possível a instalação de software sem prévia anuência nas estações individuais dos Colaboradores.

(iii) Monitoramentos

A INVESTPORT, através da sua área de TI monitora diariamente a realização de backups dos seus arquivos e redes (o servidor é completamente copiado a cada 8 horas).

Existe também, *on-line*, monitoramento de eventuais tentativas de invasão à rede da INVESTPORT e, ainda, realiza testes através de sistemas próprios para verificar se o sistema está funcionando conforme esperado, resultando relatórios informando pontos positivos e negativos encontrados.

Tais relatórios são utilizados como base para atualização das nossas prevenções e plano de resposta.

(iv) Plano de Resposta

A INVESTPORT, caso ocorra um evento envolvendo segurança cibernética, deverá iniciar o plano de resposta, conforme descrito abaixo:

Avaliação e Medidas
Uma vez identificado um evento envolvendo a segurança cibernética, o responsável pela segurança cibernética convocará reunião com a diretoria da INVETSPORT para a tomada de decisões, após ser reportado do incidente pela área de TI.
O intuito será realizar uma análise dos fatos, seus motivos e consequências imediatas, identificando a gravidade da situação.
Uma vez comprovada a realização de um incidente deve a INVESTPORT tomar medidas imediatas, que podem ser desde a publicidade do fato aos órgãos competentes como CVM, ANBIMA, COAF, etc, até mesmo informar a polícia via boletim de ocorrência ou queixa crime do fato.
Além disso, a INVESTPORT deverá definir os passos a serem tomados junto à área de TI a fim de evitar que isso ocorra novamente no futuro.

Day After
Após identificado o problema e realizadas as atitudes necessárias, serão definidas novas medidas a serem tomadas. Também deverá ser avaliado o impacto do incidente na INVESTPORT e, caso necessário, tomar as devidas ações para minimizar o risco para a empresa e seus clientes.
Todo histórico relacionado ao incidente deverá ser arquivado como evidência para eventuais esclarecimentos futuros.

(v) manter treinamento e reciclagem

A INVESTPORT mantém programa de segurança cibernética atualizado que busca atualizar seus Colaboradores de novos riscos, processos e tecnologias. O responsável pela segurança cibernética, realizará revisão deste Manual a cada 2 anos ou quando achar necessário.

Eventuais comunicações e questionamentos devem ser enviados para a área de Gestão de Riscos e de Compliance através do e-mail compliance@investport.com.br.

Em cumprimento ao art. 14, II, da Instrução CVM nº 558/15, a presente Política está disponível no endereço eletrônico da INVESTPORT: http://www.investport.com.br/.

ANEXO I AO MANUAL DE SEGURANÇA CIBERNÉTICA

6. POLÍTICAS DE SEGURANÇA

6.1 Segurança da Informação

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da INVESTPORT e às disposições deste Manual.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da INVESTPORT e circulem em ambientes externos à INVESTPORT com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais.

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 INVESTPORT. 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, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na INVESTPORT. É proibida a conexão de equipamentos na rede da INVESTPORT que não estejam previamente autorizados pela área de informática e pelos administradores da INVESTPORT.

A utilização dos ativos e sistemas da INVESTPORT, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado dos mesmos para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

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

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da INVESTPORT.

A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, raça, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

Dessa forma, o Colaborador poderá 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.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o Coordenador de Compliance.

6.2 – Monitoramento e Controle de Acesso

O acesso de pessoas estranhas à INVESTPORT a áreas restritas somente será permitida com a permissão expressa de Colaborador autorizado pelos administradores da INVESTPORT.

O acesso à rede de informações eletrônicas conta com a utilização de servidor próprio dotado de sistema para restrição de acesso via senhas e diferentes logins, de forma a segregar e impedir que informações de cada área sejam visualizadas e compartilhadas com as outras.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a INVESTPORT poderá monitorar a utilização de tais meios.

Neste sentido, a INVESTPORT:

(a) manterá diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos Colaboradores e poderá monitorar o acesso dos Colaboradores a tais pastas e arquivos com base na senha e login disponibilizados;

(b) poderá monitorar o acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos; e

(c) se reserva no direito de gravar qualquer ligação telefônica dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas disponibilizadas pela INVESTPORT para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da INVESTPORT.