MintPar

Política de Segurança Cibernética e da Informação

Esta Política é parte integrante do Manual de Operações da MintPar

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

A Política de Segurança Cibernética e da Informação da MintPar visa estabelecer regras de uso dos ativos e dos recursos da Gestora com o objetivo de minimizar riscos operacionais e estabelecer padrões de utilização das informações pertencentes a Gestora, além de mitigar os riscos de uma ameaça cibernética por meio da implementação de um programa de segurança cibernética.

I. Infraestrutura

(a) Todo equipamento possui um programa firewall de segurança para acesso a sua rede;

(b) Cada equipamento possui um programa antivírus para manter o ambiente livre de ameaças e acessos mal-intencionados;

(c) Existem dois provedores de acesso à internet e e-mail bem como de telefonia para aumentar a confiabilidade e disponibilidade de acesso aos colaboradores.

II. Controle de Acesso

A MintPar possui controle de acesso às áreas restritas. O acesso de terceiros a tais áreas somente será permitido quando acompanhado por colaborador autorizado pelos administradores da MintPar.

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos da Mint, que não poderão ser compartilhados com outras empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

A MintPar poderá monitorar a utilização de computadores, telefones, internet, e-mail e demais aparelhos, visto que tais recurso se destinam exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos colaboradores. Nesse sentido, a MintPar:

(a) Manterá diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções dos colaboradores e, com base na senha e login disponibilizados, irá monitorar o acesso dos colaboradores a tais pastas;

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

(c) Irá gravar qualquer ligação telefônica dos seus colaboradores realizada ou recebida por meio das linhas telefônicas disponibilizadas pela MintPar para a atividade profissional de cada colaborador.

(d) Cancelará imediatamente o acesso concedido a Colaboradores desligados, afastados ou que tenham função alterada na gestora.

O Diretor de Compliance é responsável por manter, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidos pela Instrução CVM 558/15, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções.

III. Segurança da informação e de dados:

(a) Não é permitida a conexão de equipamentos de informática ou software, não pertencentes à Gestora, na rede corporativa, sem a devida autorização da Diretoria ou do gerente responsável pela área juntamente com a anuência técnica do departamento de TI;

(b) O departamento de TI deve efetuar verificações semestrais na rede corporativa, para validar o acesso seguro aos recursos disponíveis;

(c) As irregularidades encontradas durante essas verificações devem ser comunicadas à Diretoria da MintPar.

(d) O bloqueio de acesso à rede será efetuado pelo departamento de TI sempre que solicitado pela Diretoria, ou caso seja detectado algum risco para

a rede ou para os sistemas da Gestora.

(e) 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.

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

IV. Backup e Restore de Arquivos

(a) Para a garantia do backup das informações da Gestora, estas devem ser armazenadas nos servidores da rede corporativa;

(b) Não haverá garantia de backup para arquivos armazenados nas estações de trabalho (desktops ou notebooks);

(c) O backup de dados nos servidores da rede corporativa deve ser automatizado e periódico, de acordo com os procedimentos de backup e restore definidos pelo departamento de TI;

(d) O restore de dados deve ser solicitado ao departamento de TI e será realizado de acordo com os procedimentos específicos do mesmo;

(e) As mídias de backup e as cópias de segurança devem ser armazenadas em local apropriado. A cópia de segurança deverá ser armazenada fora da Gestora, sendo auditadas periodicamente; e

(f) As mídias (suprimentos) serão adquiridas pela MintPar, sempre que necessário.

V. Segurança Cibernética

Com o objetivo mitigar os riscos de uma ameaça cibernética, a MintPar adota medidas de prevenção por meio da implementação de um programa de segurança cibernética que contempla os seguintes aspectos: (i) identificação e avaliação dos riscos internos e externos aos quais a MintPar está sujeita, os ativos de hardware e software e os processos que precisam de proteção; (ii) estabelecimento de ações de prevenção e proteção; (iii) monitoramento das ameaças em tempo hábil; (iv) criação de um plano de resposta; e (v) reciclagem e revisão do programa de segurança cibernética.

O Diretor de Compliance e Risco será o responsável para tratar e responder questões relacionadas à segurança cibernética. Qualquer processo ou ativo classificado como Informação Confidencial será considerado como vulnerável para fins de segurança cibernética, sendo classificado internamente com alto grau de ameaça institucional em caso de eventual ataque cibernético.

Nesse sentido, o Compliance realiza ações de prevenção e proteção de tais ativos, por meio dos procedimentos elencados na Política de Segurança Cibernética e da Informação. Adicionalmente, ressalta-se que a MintPar trabalha com (i) backup dos seus arquivos; (ii) sistema de firewall e antivírus; (iii) restrição de instalação e execução de softwares e aplicações não autorizadas por meio de controles de execução de processos; e (iv) acesso restrito a páginas na rede mundial de computadores.

Para fins de monitoramento, o Diretor de Compliance e Risco da MintPar realiza, periodicamente, testes de segurança e procedimentos para detectar falhas e vulnerabilidades. Adicionalmente, a MintPar (i) mantém inventários atualizados de hardware e software por ela detidos; (ii) mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizados; (iii) monitora diariamente as rotinas de backup, executando testes regulares de restauração dos dados; e (iv)

analisa regularmente as trilhas de auditoria criadas, de forma a permitir a rápida identificação de ataques, sejam internos, sejam externos.

No caso concreto de um ataque cibernético amplo nas redes da MintPar, o Compliance deverá contatar imediatamente os Colaboradores da MintPar, bem como Gestora especializada para resolver a questão no menor tempo possível. Neste cenário, os Colaboradores deverão utilizar instalações de contingência até a normalização dos serviços, as quais obedecerão às regras de controle de acesso previstas na Política de Segurança da Informação. Em se tratando de um ataque individual a um determinado Colaborador, a MintPar deverá disponibilizar novos equipamentos para a continuidade da prestação dos serviços por parte daquele Colaborador.

Todo e eventual incidente cibernético deverá ser documentado por escrito em relatório elaborado pelo Compliance, no qual constarão as descrições do incidente e as medidas tomadas para resolver tal incidente, e deverá ser arquivado na sede para fins de evidência para eventuais questionamentos.

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.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais. Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora, aos seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Gestora, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo Diretor de Compliance.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora e de seus clientes. 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.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Gestora.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão. O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores devem se abster de utilizar hard drives, pen-drives, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora.

É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de compliance. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também

terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da Gestora.

Em nenhuma hipótese um Colaborador pode emitir opinião por e-mail em nome da Gestora, ou utilizar material, marca e logotipos da Gestora para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

O Diretor de Compliance também monitorará e, será avisado por e-mail em caso de tentativa de acesso aos diretórios e logins virtuais no servidor protegidos por senha. O diretor de compliance elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na Gestora. Não é permitida a instalação de nenhum software ilegal ou que possua direitos autorais protegidos. A instalação de novos softwares, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos Colaboradores para aspectos profissionais e pessoais.

A Gestora se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Gestora para a atividade profissional de cada Colaborador. O diretor de compliance é encarregado de, periodicamente, monitorar, por amostragem, as ligações e demais comunicações realizadas pelos Colaboradores. Qualquer informação suspeita encontrada será esclarecida imediatamente pelo diretor de compliance.

Todas as informações e conteúdos produzidos e/ou alterados na Gestora ficam armazenadas em servidor local, com uma cópia de segurança armazenada em fita de backup em uma localidade externa à Gestora. O servidor da Gestora é protegido por firewall e programas antivírus, assim como cada uma das estações de trabalho individuais.

Em caso de divulgação indevida de qualquer informação confidencial, o diretor de compliance irá apurar o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador.

VI. Procedimentos internos para tratar eventual vazamento de informações confidenciais, reservadas ou privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Mint, na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de Compliance deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, o Diretor de Compliance, primeiramente, identificará se a Informação vazada refere-se ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, o Diretor de Compliance procederá da seguinte forma:

1. No caso de vazamento de Informações relativas aos fundos de investimento geridos:

   Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou

uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

2. No caso de vazamento de Informações relativas aos cotistas:

   Neste caso, ao Diretor de Compliance procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, o Diretor de Compliance ficará à inteira disposição para auxiliar na solução da questão.

Os procedimentos previstos nesta Política de Segurança Cibernética, conforme mencionados anteriormente, serão revisados anualmente pela MintPar, ou quando houver alteração na regulação referente à segurança cibernética. Em tais revisões, serão atualizadas as avaliações de riscos, vulnerabilidades e ameaças identificadas originalmente.