POLÍTICA DE SEGURANÇA CIBERNÉTICA

I. OBJETO

Esta política tem por objeto estabelecer as regras, procedimentos e controles de segurança cibernética aplicáveis à Trigger Gestora de Recursos Ltda. ("Trigger"), com o objetivo de assegurar e aprimorar a confidencialidade, a integridade, a disponibilidade e a privacidade dos dados e dos sistemas de informação utilizados pela Trigger. As regras previstas nesta política foram estruturadas de acordo com o porte, perfil de riscos, modelo de negócio e a complexidade das atividades desenvolvidos pela Trigger.

Esta política se aplica a todos os colaboradores da Trigger.

II. AVALIAÇÃO DE RISCOS

Os seguintes ativos da Trigger precisam de proteção relacionada a segurança cibernética, sem prejuízo de outros que venham a ser identificados pelos colaboradores da Trigger:

- Dados e informações: as informações confidenciais da Trigger e relacionadas à atuação da Trigger, incluindo informações a respeito dos fundos de investimento cuja gestão foi atribuída à Trigger, carteiras geridas pela Trigger, investidores, colaboradores, operações e ativos investidos pelos fundos de investimento sob sua gestão, bem como de comunicações internas e externas, em qualquer meio (inclusive eletrônicas e físicas).
- Sistemas: as informações confidenciais sobre os sistemas utilizados pela Trigger.
- Processos e controles: as informações confidenciais sobre os processos e controles internos que sejam parte da rotina das áreas de gestão de recursos e compliance da Trigger.
- Equipamentos: computadores e notebooks usados pelos colaboradores da Trigger em suas atividades na Trigger, que podem conter informações confidenciais.

Foram identificados os seguintes principais riscos de segurança cibernética, sem prejuízo de outros que venham a ser identificados pelos colaboradores da Trigger:

- Malware: softwares desenvolvidos para corromper computadores e redes.
- Engenharia social: métodos de manipulação para obter informações confidenciais (inclusive *pharming*, *phishing*, *vishing* e *smishing*).
- Ataques de DDoS (distributed denial of services) e botnets: ataques visando a negar ou a atrasar o acesso aos serviços ou sistemas da instituição.
- Invasões (advanced persistent threats): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

De forma a orientar e aprimorar os mecanismos e controles de segurança cibernética, todos os colaboradores da Trigger deverão, periodicamente, identificar os riscos internos e externos e os ativos que precisam de proteção.

III. PROTEÇÃO E PREVENÇÃO

Serão adotadas as seguintes medidas para mitigar os riscos identificados, para prevenir a ocorrência de incidentes cibernéticos, incluindo a programação e implementação de controles, inclusive os descritos a seguir:

(i) Disponibilização e uso dos recursos de TI:

Os colaboradores utilizarão computadores, recursos computacionais e sistemas disponibilizados pela própria Trigger, sendo que a utilização de notebooks e máquinas próprias deverá ser previamente autorizada pela Trigger, sujeita à avaliação da segurança do equipamento e implementação de medidas de segurança.

Os computadores, recursos computacionais e sistemas se destinam apenas a fins profissionais, devendo o uso para fins pessoais ser evitado por todos os colaboradores.

(ii) Controle de acesso:

O acesso de cada colaborador aos recursos e sistemas será individualizado, por meio de perfis de acesso, que segregam as funções realizadas pelas diversas áreas da Trigger e controlam os privilégios, credenciais e níveis de acesso aplicáveis a cada uma delas.

Há diferentes níveis de acesso a pastas e arquivos eletrônicos, em especial aqueles que contêm informações confidenciais, que são atribuídos a cada colaborador, de acordo com suas funções e responsabilidades.

Colaboradores afastados ou desligados terão seus acessos imediatamente cancelados. Colaboradores que tenham sua função alterada dentro da Trigger terão seus acessos atualizados para compatibilização com a nova função.

A Trigger poderá monitorar o acesso às pastas e aos arquivos, com base na senha e login disponibilizados aos colaboradores.

(iii) Senhas:

Senhas de caráter sigiloso, pessoal e intransferível, serão fornecidas a cada um dos colaboradores para acesso aos computadores, à rede corporativa e ao correio eletrônico corporativo. As senhas não deverão ser transmitidas por cada um dos colaboradores a quaisquer terceiros.

IV. MONITORAMENTO E TESTES PERIÓDICOS

Para supervisionar os riscos identificados e verificar e assegurar a efetividade das medidas de prevenção e proteção adotadas pela Trigger, bem como para identificar eventuais incidentes, detectar as ameaças

em tempo hábil e, caso necessário, reforçar os seus controles, poderão ser testes periódicos no ambiente de TI, com a geração de relatórios de indicadores e históricos.

Os relatórios poderão incluir indicadores e históricos: (i) de períodos de indisponibilidade no acesso à internet e aos sistemas críticos; (ii) do tempo de resposta no acesso à internet; (iii) de incidentes de segurança; e (iv) da atividade dos colaboradores (inclusive sites visitados, e-mails recebidos e enviados, upload/download de arquivos, entre outros).

Para possibilitar a gestão segura e confiável das informações e dados relacionados às suas atividades, bem como para permitir a realização de auditoria e testes sobre os seus mecanismos de controle e prevenção, a Trigger poderá: (i) manter cópias de segurança das mensagens de correio eletrônico e outras comunicações realizadas pelos colaborados por meio de seus sistemas, equipamentos e servidores; (ii) monitorar e gravar conversas telefônicas e virtuais; e (iii) manter *backups* de todas as informações e dados mantidos em meios eletrônicos.

V. RESPOSTAS A INCIDENTES

Caso um incidente de segurança seja identificado, a Trigger realizará uma avaliação inicial sobre a extensão e gravidade do ocorrido, bem como sobre os seus motivos e consequências imediatas.

A avalição deverá ponderar, inclusive: (i) se houve prejuízo para a Trigger ou algum terceiro; (ii) se haverá comunicação interna ou externa, em especial a indivíduos que tenham sido afetados; (iii) se há a necessidade de informar à CVM, ANBIMA ou alguma autoridade sobre o ocorrido; (iv) se há a necessidade de registro de boletim de ocorrência ou queixa crime a respeito do ocorrido; e (v) se há a necessidade de envolver consultores especializados externos, inclusive consultores de segurança cibernética e assessores legais.

Após a avaliação inicial do ocorrido e conforme sua gravidade, a Trigger poderá implementar medidas para contornar o incidente e retornar ao modo normal das operações, inclusive: (i) iniciar a redundância de TI; (ii) redirecionar as linhas de telefone para os celulares; (iii) instruir o provedor de Telecom a desviar linhas de dados/e-mail; (iv) reconstrução de eventuais sistemas; e (v) alterações nas medidas de prevenção e proteção.

Todos os colaboradores deverão reportar incidentes diretamente ao Responsável pela Segurança Cibernética ou por meio do canal de reporte de incidentes que será informado a todos os colaboradores.

VI. RESPONSABILIDADE

O Diretor responsável pela gestão de riscos da Trigger, nos termos do art. 4º, inciso V e §7º, da Resolução CVM n.º 21/2021, será o responsável pelo acompanhamento do cumprimento desta Política, inclusive para tratar e responder questões de segurança cibernética, com o auxílio da área de TI e de assessores externos especializados.

VII. VIOLAÇÃO

O colaborador que violar as disposições desta política e as normas aplicáveis à segurança cibernética estará sujeito a penalidades, a serem definidas de acordo com a natureza e a gravidade da violação, pela administração da Trigger.

Sem prejuízo da aplicação das sanções previstas na legislação e regulamentação aplicáveis, os colaboradores que descumprirem as regras previstas nesta Política estarão sujeitos às seguintes sanções, a serem definidas pela administração da Trigger, de acordo com a natureza e a gravidade da violação:

- advertência;
- suspensão;
- demissão de colaborador que seja empregado ou estagiário;
- destituição de colaborador que seja diretor; ou
- exclusão de colaborador que seja sócio (desde que respeitado o quórum de aprovação e procedimento previstos no contrato social da Trigger).

Nas hipóteses em que a Trigger venha a ser responsabilizada por infrações legais ou regulamentares eventualmente praticadas por seus colaboradores, a Trigger se reserva o direito de pleitear indenização pelos danos eventualmente incorridos, incluindo os danos de imagem e reputacionais.

VIII. ATUALIZAÇÃO

Esta política de segurança cibernética será continuamente atualizada, para que haja a constante reavaliação dos ativos, dos riscos e dos procedimentos de supervisão e respostas a incidentes da Trigger.

* * *