Política de Segurança Cibernética

Nós, da CM Capital, sabemos que parte importante da excelência de nossos serviços é a proteção de dados e informações relativas aos investimentos de nossos Clientes ("Dados"). Neste sentido, tomamos precauções, dentro dos mais altos padrões comerciais, a fim de garantir a segurança de tais informações, respeitando, ainda as leis e normas aplicáveis a nossas atividades. Apontamos ainda que adotamos todas as leis e regulações aplicáveis e padrões de segurança iguais ou superiores aos adotados no mercado.

A Política de Segurança Cibernética ("Política") da CM Capital tem como objetivo atender ao disposto na Resolução CMN nº 4.658 de 26 de abril de 2018, bem como transmitir os princípios de Segurança Cibernética que guiam nosso trabalho e os mecanismos de controle utilizados tanto para a prevenção como para o combate e tratamento de eventuais incidentes de Segurança Cibernética.

Assim, o presente documento apresenta um resumo dos principais pontos e diretrizes de segurança que abordamos em nossa Política de Segurança Cibernética.

1. DEFINIÇÕES

- ✓ **Riscos Cibernéticos:** são os riscos de ataques cibernéticos, oriundos de *malware*, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas da CM Capital, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades da CM Capital.
- ✓ **Serviços Relevantes:** Serviços prestados por Prestadores de Serviço à CM Capital cuja indisponibilidade, vulnerabilidade ou inconsistência possa prejudicar a continuidade de seus negócios: (i) afetando o atendimento ofertado ao Cliente; (ii) paralisando a operação da CM Capital, podendo causar perdas financeiras; ou (iii) impedindo o fornecimento de informações pela CM Capital aos entes reguladores e/ou o cumprimento de direitos e garantias dos clientes.
- ✓ **Incidentes:** Qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma

violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis. São considerados incidentes, mas não se limitando a esses: (i) acesso indevido a contas e/ou sistemas da CM Capital; (ii) acessos não autorizado a bases de Dados ou Informações de uso interno ou confidencial da CM Capital; (iii) alteração ou perda de Dados ou Informações, ou de acesso a sistemas ou ambientes lógicos, bem como da integridade destes; (iv) vulnerabilidades existentes nos sistemas, bem como situações de indisponibilidade dos sistemas e/ou das informações ou (v) demais falhas de segurança que acarretem em acessos não autorizados a sistemas ou ambientes tecnológicos da CM Capital, por meio de técnicas, conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

2. MEDIDAS DE SEGURANÇA E PREVENÇÃO

- ✓ **Classificação de informações**: Classificamos os dados em níveis de confidencialidade, de acordo com a natureza e a criticidade das informações tratadas, restringindo os níveis de acesso e reforçando os mecanismos de controle e segurança de acordo com a criticidade e sensibilidade de cada dado.
- ✓ **Equipamentos e Estrutura:** Os equipamentos utilizados para o desenvolvimento das atividades da CM Capital devem estar sempre atualizados, regra que inclui sistema operacional, antivírus e firewalls, garantindo assim maior proteção às informações neles inseridas. Ainda, os cuidados se estendem também à infraestrutura onde são armazenados os dados: que possuem cópias de segurança (backups) atualizadas periodicamente, conforme os padrões de segurança mais altos disponíveis no mercado.
- ✓ **Armazenamento de Dados e Computação em Nuvem:** Os serviços de armazenamento de dados e computação em nuvem que contratamos passam por uma seleção interna rígida que avalia a necessidade da terceirização do serviço em questão e a confiabilidade técnica do fornecedor analisado, a fim de garantir que ele possua as qualificações de segurança necessárias. Ainda, são cumpridos todos os requisitos previstos na regulamentação específica, em especial a Resolução nº 4.658/2018 do Conselho Monetário Nacional.
- ✓ **Obtenção de Credenciais e Gerenciamento de Acesso:** Os nossos colaboradores e prestadores de serviço assumem rígidos compromissos de confidencialidade e compliance ao obterem as credenciais que dão acesso aos nossos dados confidenciais ou a dados classificados como sensíveis pela CM Capital. Estas credenciais, por sua vez, são atualizadas periodicamente, em conformidade com as regulações e normas

aplicáveis. Ainda, o acesso aos dados é restringido a menor permissão e privilégio possíveis, possuindo a CM Capital capacidade para monitorar e registrar o acesso a dados classificados como sensíveis, sendo exigida a mesma garantia de seus prestadores de serviço.

- ✓ **Capacitação e Atualização:** Os nossos colaboradores passam por treinamentos periódicos referentes à prevenção e resposta à incidentes, bem como de melhores práticas de segurança cibernética, sendo realizadas ainda, avaliações buscando atingir o maior comprometimento de todos os nossos colaboradores. Além disso, disponibilizamos canais internos pelos quais os colaboradores possam encaminhar denúncias e suspeitas de fragilidades e violações de segurança cibernética, a fim de agilizar assim a resposta do time especializado a eventuais incidentes.

3. INCIDENTES DE SEGURANÇA

Visando garantir a continuidade de nossas atividades em caso de eventuais incidentes de segurança cibernética, realizamos, constantemente, testes de continuidade de negócios, a fim de:

- ✓ Diagnosticar possíveis falhas em nossos sistemas;
- ✓ Garantir que nossos serviços continuem disponíveis;
- ✓ Restaurar os serviços o mais breve possível em caso de interrupção; e
- ✓ Aperfeiçoar os métodos de armazenamento e gerenciamento de informações e dados dos clientes.

Assim, após a identificação de possíveis fragilidades efetuamos todas as adequações e alterações necessárias para que a nossa segurança seja mantida.

Caso seja identificado incidente de segurança cibernética o time de resposta deverá ser acionado de acordo a criticidade do incidente.

Na ocorrência de incidentes relevantes, a alta administração e a Supervisão de Relações com o Mercado e Intermediários(SMI) da CVM, serão comunicados após confirmado a materialização do incidente relevante, em toda a sua extensão, e estabelecido planos de ação para mitigá-lo.