MELHORES PRÁTICAS DE UTILIZAÇÃO DE RECURSOS COMPUTACIONAIS e SEGURANÇA DA INFORMAÇÃO

A CM Capital Markets (“CM Capital” ou “Companhia”) está comprometida a tratar dados e informações, sejam de seus clientes, colaboradores, fornecedores, parceiros e terceiros, com o mais alto nível de cuidado, confidencialidade e conformidade com a legislação aplicável.

Com este objetivo e seguindo as melhores práticas de utilização de recursos computacionais e segurança da informação, a CM capital aplica em seu ambiente e seus funcionários os referidos procedimentos. Tais aplicações visam por fim oferecer aos nossos clientes um padrão de excelência no que diz respeito às melhores práticas legais e de conduta ética.

No decorrer deste documento, apresentaremos os procedimentos e práticas adotadas pela CM Capital no tocante a segurança da informação e segurança cibernética, bem como recomendações de segurança da informação e cibernética para nossos clientes no acesso aos sistemas fornecidos pela CM Capital.

1. Sigilo e Segurança da informação

A CM Capital Markets possui recursos e procedimentos para prover o sigilio e segurança das informações trafegadas na CM Capital Markets, estes procedimentos têm como objetivo proteger as informações de nossos clientes e da empresa, controlando o risco de divulgação ou alteração por pessoas não autorizadas. Apesar da aplicação das tecnologias, procedimentos e softwares não garantirem total imunidade a falhas ou ataques eletrônicos, suas aplicações mitigam os riscos em grande escala.

No que tange a questões referentes à sigilo e segurança da informação, podemos destacar:

- **Firewall:** Ferramenta que estabelece regras e filtros de tráfego de informações entre seu computador e a CM Capital, utilizados como defesa contra ameaças externas e invasores (hackers, crakers etc). Essas ferramentas também são responsáveis em garantir a segurança na transmissão de suas ordens de negociação para a B3.

- **Links de Internet:** A CM Capital possui acesso de Internet totalmente contingenciado, com links físicos de acesso de operadoras e caminhos distintos. Possuímos também um site de contingência externo localizado em outro prédio, onde todas as informações são replicadas para atendimento ao Plano de Continuidade do Negócio, garantindo a integridade e segurança dessas informações.

- **Antivírus:** A CM Capital possui antivírus robusto e atualizado para detectar e eliminar potenciais vírus(programas danosos), assim como atua bloqueando a instalação e propagação do programa malicioso.

- **Monitoramento:** Além das ferramentas utilizadas para proteger o ambiente da CM Capital e informações de seus clientes, monitoramos em tempo real o ambiente tecnológico com o objetivo de identificar possíveis falhas.

2. Recomendações de Segurança da informação e Cibernética

Assim como a CM Capital Markets, nossos clientes também desempenham um papel de grande importância no processo de proteção de suas próprias informações. Assim entendemos que os clientes devem estabelecer e garantir os mínimos padrões necessários de infraestrutura e procedimentos para preservação e garantia dos interesses comuns.

Indicamos a seguir alguns cuidados a serem tomados por nossos clientes com relação a segurança da informações e cibernética no acesso aos sistemas disponibilizados pela CM Capital Markets.

- **Composição, Guarda e Troca de Senha:** Escolha senhas difíceis de serem descobertas, evite datas comemorativas e números com sequências simples, como 123456, não anote e não compartilhe suas senhas com ninguém, nós da CM Capital Markets não solicitamos sua senha em nenhuma ocasião.

- **Utilização de Acessos:** As credenciais de acesso devem ser de uso exclusivo dos usuários aos quais os acessos foram atribuídos. Não recomendamos e/ou autorizamos em qualquer hipótese o compartilhamento dos acessos fornecidos pela CM Capital Markets.

- **Uso da Internet:** Certifique-se que sua conexão é segura, principalmente quando envolver dados confidenciais. Para isso verifique se o cadeado de segurança está ativo no seu browser (navegador). Cuidado ao utilizar conexões wireless(Wi-Fi) redes públicas, elas também podem ser utilizadas para comprometer seus dados pessoais.

- **Atualização de Softwares:** Manter os softwares atualizados é uma boa prática, com isso recomendamos que mantenha seu computador atualizado com a última versão do sistema operacional e seus programas de segurança, tais como antivírus e Firewall pessoal.

- **Segurança no uso de Computadores e Dispositivos Móveis:** Bloqueie sua tela, use um código de bloqueio ou biometria para evitar que outras pessoas utilizem o seu aparelho, principalmente em caso de perda ou roubo. Habilite o recurso de proteção por senha nos aplicativos de Mensagens, Investimentos e outros.

- **Sistemas de Antivírus e Antispyware:** A utilização de sistemas antivírus e antispyware, ajuda a manter o parque tecnológico protegido quanto a ameaças eletrônicas que podem inviabilizar a utilização parcial ou completa de recursos computacionais. Essas ameaças também oferecem vulnerabilidade a ataques ou falhas.