POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Corretora atendendo às disposições da Resolução CMN/BACEN 4.893, de 26 de fevereiro de 2.021, elaborou a sua Política de Segurança Cibernética, formulada com base em princípios e diretrizes que buscam assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Essa Política é compatível com o porte, o perfil de risco, o contexto operacional da instituição, a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da Corretora, a sensibilidade dos dados e das informações sob nossa responsabilidade.

A Dascam Corretora de Câmbio Ltda. opera no mercado cambial de uma forma extremamente conservadora. Sua atuação é focada apenas na intermediação nas operações de câmbio de seus clientes. Não realiza operações com posição própria, bem como, turismo e não tem correspondentes cambiais. Concentra-se, principalmente, no assessoramento técnico, sua especialidade.

Diretoria – Responsável pela aprovação e manutenção da Política de Segurança Cibernética, por assegurar que a estrutura está devidamente implementada e é apropriada para suas atividades, provendo-a com recursos adequados.

Diretor Responsável – Diretor indicado a representar a Corretora junto ao Banco Central do Brasil, responsável por definir as políticas e objetivos gerais e respaldar a Diretoria com informações relevantes acerca da Política de Segurança Cibernética.

Resumo da Política:

A política de segurança cibernética contempla:

I - Os objetivos de segurança cibernética da instituição;

II - Os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética;

III - Os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;

IV - O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;

V - As diretrizes para:

a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;

c) a classificação dos dados e das informações quanto à relevância; e

d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; e

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

VII - as iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com as demais instituições do segmento.

Na definição dos objetivos de segurança cibernética, foi observada a capacidade da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Os procedimentos e os controles de que trata o inciso II abrangem, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

Os procedimentos e os controles citados no inciso II são aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição.

O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, citados no inciso IV, abrangem inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

As diretrizes de que trata o inciso V, alínea "b", contemplam procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição.

Assim a Corretora em cumprimento às disposições da Resolução CMN/BACEN 4.893, de 26 de fevereiro de 2.021, elaborou a Política de Segurança Cibernética em total consonância com as disposições regulamentares e as melhores práticas de mercado, considerando o seu contexto operacional.

A Diretoria está plenamente engajada no processo, definiu e aprovou a política, disponibilizou adequados recursos humanos e materiais. É responsável pelas informações e promoveu ampla divulgação aos clientes, colaboradores e prestadores de serviços em seu sítio na rede mundial de computadores.