POLÍTICA DE SEGURANÇA CIBERNÉTICA E PLANO DE RESPOSTA À INCIDENTES

FAIR CORRETORA DE CÂMBIO S/A
Janeiro/2026

POLÍTICA DE SEGURANÇA CIBERNÉTICA E PLANO DE RESPOSTA A INCIDENTES

1. Objetivo e Abrangência

Esta política estabelece as diretrizes de segurança da informação para proteger a Fair Corretora, seus clientes, colaboradores, parceiros e fornecedores.

Esta política tem como objetivo mitigar a ocorrência de falhas sistêmicas, manter a integridade e sigilo de dados, bloquear acessos indevidos/não autorizados e garantir a segurança, protegendo a corretora contra riscos cibernéticos e tecnológicos, garantindo assim a continuidade dos sistemas e operações, mesmo diante de incidentes e imprevistos. Além de cumprir com as regulamentações locais e internacionais relacionadas à segurança e privacidade de dados.

2. Controles Internos

Esta política estabelece controles internos para mitigar riscos, sendo eles:
- Controle de acesso: Apenas usuários autorizados terão acesso aos sistemas e dados críticos.
-Criptografia: Proteção de dados confidenciais durante a transmissão e no armazenamento.
- Backups e redundância: Implementação de processos regulares de backup de dados e sistemas críticos, com planos de recuperação de desastres.
- Monitoramento contínuo: Utilização de ferramentas de monitoramento de segurança para detectar intrusões ou falhas nos sistemas em tempo real.
- Treinamento de funcionários: Capacitação de todos os colaboradores sobre as boas práticas de segurança da informação e como lidar com incidentes.

3. Governança de Sistemas Terceirizados

A responsabilidade final pela segurança dos dados permanece com a Corretora. Os contratos com fornecedores de sistemas de câmbio devem exigir:

- **Segregação de Funções:** Bloqueio sistêmico para impedir que o mesmo usuário insira e liquide a mesma operação de câmbio.
- **Notificação de Incidentes:** Obrigação contratual do fornecedor de notificar a Corretora sobre qualquer incidente em até **2 horas**.

4. Rastreabilidade e Auditoria (CMN 5.274)

Todos os sistemas — internos ou terceirizados — devem registrar logs imutáveis contendo: IP de origem, usuário, ID da operação.

5. Procedimento Rápido de Resposta a Incidentes

Fluxo de Execução Imediata (4 Fases)

[1. DETECÇÃO] ----> [2. CONTENÇÃO] ----> [3. ERRADICAÇÃO] ----> [4. RECONCILIAÇÃO e NOTIFICAÇÃO]

Fase 1: Detecção e Triagem: o alerta pode vir do antivírus, de comportamento anômalo do usuário ou de uma notificação do fornecedor do sistema.

- **Ação da TI:** Identificar a origem. O problema é local (computador de um operador) ou no sistema terceirizado de câmbio?

Fase 2: Contenção: bloquear o avanço da ameaça para proteger a base de dados da Corretora.

- **Em caso de ataque local:** isolar a máquina afetada da rede imediatamente e bloquear o usuário no Servidor, derrubando todas as sessões ativas dele nos sistemas.
- **Em caso de ataque em Sistema Terceirizado:** revogar temporariamente as credenciais e chaves de API que conectam a Corretora ao sistema afetado, suspender temporariamente negociações na plataforma afetada.

Fase 3: Erradicação e Recuperação: executar procedimento de *restore.*

- **Ação da TI:** Formatar/restaurar a máquina afetada a partir de *backup's* e dados dos servidores de *mirror*.
- **Ação com Terceiro:** Exigir o laudo técnico do fornecedor comprovando que a vulnerabilidade no sistema foi corrigida antes de reestabelecer as conexões de API.

Fase 4: Reconciliação e Notificação Regulatória

- **Auditoria de Operações:** O setor de compliance devem auditar todos os contratos de câmbio gerados no dia do incidente para garantir que nenhum dos seus dados tenham sido adulterados.
- **Comunicação ao BCB:** Se o incidente causou interrupção relevante dos serviços ou vazamento de dados de clientes, a diretoria deve notificar o Banco Central do Brasil em até **24 horas** do diagnóstico.

6. Considerações Finais

A política de segurança cibernética e o plano de resposta a incidentes da Fair Corretora de Câmbio serão revisados anualmente com o objetivo de garantir a sua abrangência, efetividade e atualização de forma contínua, envolvendo não apenas a implementação de tecnologias avançadas de segurança, mas também o treinamento adequado dos funcionários e a adaptação às regulamentações do mercado financeiro, de forma a garantir a proteção tanto dos dados da empresa quanto dos clientes, além de assegurar a conformidade com as obrigações legais e regulatórias em vigor.