Webinar
Atualizações Roteiro PQO

16/05/2023

Histórico

- Atualização com base na Consulta Pública Restrita, Nota de Orientação da BSM e inclusão do item de teste de estresse de liquidez.

Agenda

i. Item Portabilidade

ii. Mecanismo de Prevenção a Fraude e Segurança Cibernética

iii. Teste de Estresse de Liquidez

iv. Itens de Tecnologia

v. Itens Excluídos

vi. Plano de Implementação

vii. Q&A

Item Portabilidade

Audiência Pública Restrita

Atualização Item 71 – O Participante deve realizar a transferência dos valores mobiliários, bem como dos eventuais direitos e ônus a eles atribuídos, no prazo máximo de 2 (dois) dias úteis contados do recebimento, pelo Participante, do requerimento válido formulado pelo Cliente, sendo observados, em qualquer hipótese, os procedimentos operacionais aplicáveis.
Para as solicitações de transferência de valores mobiliários (STVM) que não forem atendidas no prazo máximo de 2 (dois) dias úteis, o Participante deve:

71.1. Informar ao Cliente caso o pedido de transferência não possa ser implementado em razão de inconsistências ou incompletudes no preenchimento da STVM, da não conformidade da documentação enviada ou da necessidade de prazo adicional para o Participante analisar a documentação enviada pelo Cliente, no prazo de 2 (dois) dias úteis, a contar da data do recebimento, pelo Participante, do requerimento formulado pelo Cliente.

71.1.1 O procedimento adotado pelo Participante deve contemplar medidas de interação tempestiva e frequente junto ao Cliente a cada 2 (dois) dias úteis, quando da necessidade de análise adicional pelo participante, a contar da data do recebimento, pelo Participante, do requerimento formulado pelo Cliente, mantendo os registros e evidências dessas interações pelo prazo determinado na regulação vigente.

Item Portabilidade

Audiência Pública Restrita

71.1.2 O procedimento deve ainda prever que o investidor tenha acesso, a qualquer tempo, sobre a atual situação do pedido de transferência e dos motivos de sua não implantação até aquele momento.

Item Portabilidade

Audiência Pública Restrita

Atualização Item 75 - O Participante deve dispor de meios eletrônicos para tratar os controles de tempo e aceitação (recepção, tratamento e efetivação) dos pedidos de portabilidade dos valores mobiliários (exceto derivativos) em custódia de seus Clientes, observando as seguintes regras:

75.1. Deve estar apto a receber pedidos eletrônicos de portabilidade de seus Clientes através da Área do Investidor da B3 ou de sistema desenvolvido pelo próprio Participante e conectado aos sistemas da B3 para realizar o devido tratamento junto aos sistemas da central depositária da B3;

75.1.1 O meio disponibilizado pelo Participante deve ser capaz validar automaticamente, no mínimo, as informações de conta e ativos para mitigar eventuais inconsistências ou incompletudes nas solicitações da portabilidade;

75.1.2 O investidor deve poder consultar, a qualquer momento, a situação atual do seu pedido de transferência através do meio eletrônico disponibilizado pelo Participante;

Item Portabilidade

Audiência Pública Restrita

75.2. Nos termos da Resolução CVM 32/2021, a transferência dos valores mobiliários a outro custodiante deve obedecer a procedimentos razoáveis, tendo em vista as necessidades dos investidores e a segurança do processo, e deve ser efetuada em, no máximo, 2 (dois) dias úteis contados do recebimento, pelo custodiante, do requerimento válido formulado pelo investidor;

75.3. O procedimento previsto no item 75 vigorará a partir de 02/01/2024 e será aplicável apenas aos Participantes que tenham mais de 10 mil clientes pessoa física com posição junto à central depositária da B3 no último dia útil do ano anterior ao período em que será observado o cumprimento dessa regra.

Mecanismo de Prevenção a Fraude e Segurança Cibernética | Capítulo 3 – Executar Ordens

Nota de Orientação BSM

Inclusão Item 26- O Participante deve dispor de período de suspensão da execução de ordem suspeita (holding period) de seus clientes, quando da identificação de acessos e operações em cenários de risco.

Mecanismo de Prevenção a Fraude e Segurança Cibernética | Capítulo 1 – Cadastrar Clientes

Nota de Orientação BSM

Atualização Item 1- No relacionamento com o Cliente, o Participante deve observar o disposto em suas Regras e Parâmetros de Atuação, que devem conter, obrigatoriamente, os procedimentos adotados no que se referem a:

1.16. procedimentos adotados pelo Participante para o processo de KYC

Mecanismo de Prevenção a Fraude e Segurança Cibernética | Capítulo 9 – Prevenção a Fraude e à Lavagem de Dinheiro

Nota de Orientação BSM | **Audiência Pública Restrita**

Atualização Item 113 - O Participante deve monitorar continuamente as seguintes operações ou situações envolvendo títulos ou valores mobiliários:

113.1.6: Padrão(ões) de acesso e de operação de seus clientes, por meio de trilhas de auditoria que contemplem o registro de origem de ordem, de acesso e/ou de cadastro, contemplando no mínimo cenários de risco; e consequentemente, avaliar os casos em que a origem da ordem não condiz com o padrão comumente adotado para o acesso do cliente;
13.1.7: grupos de clientes e pessoas vinculadas ao Participante que insiram ordens a partir da mesma origem; (ii) de clientes que compartilhem dados cadastrais como logradouro, procurador, emissor de ordens, telefone, e-mail entre outros;
113.1.8 ordens enviadas de uma mesma origem e de clientes com cadastro efetuado a partir de uma mesma origem;
113.1.9 operações coordenadas em que a mesma origem de ordem é utilizada por dois ou mais clientes; e/ou
113.1.10 cadastros recentes realizados no sistema do Participante a partir das origens das ordens enviadas já mapeadas como de risco pelo Participante.

Mecanismo de Prevenção a Fraude e Segurança Cibernética | Capítulo 12 – Segurança das Informações

Atualização Item 121 - O Participante deve estabelecer e difundir, entre todos os seus colaboradores, Prepostos e prestadores de serviço com acesso a dados ou a informações sensíveis, os documentos que compõem a política de segurança da informação aprovada pela alta administração, que contenham, no mínimo, as seguintes diretrizes:

121.10. Implementar, manter e monitorar uma política de senha, considerando as características do seu negócios e as melhores práticas de mercado, para garantir que os usuários internos e externos (clientes) criem senhas que protejam seus dados e evitem ataques cibernéticos. No caso de sistemas transacionais acessados via homebroker web, homebroker app e via acesso mobile, a política deve prever a utilização de segundo fator de autenticação.

Mecanismo de Prevenção a Fraude e Segurança Cibernética | Capítulo 12 – Segurança das Informações

Nota de Orientação BSM

Atualização Item 122 - O Participante deve manter e monitorar a segurança da rede, de arquivos, da base de dados, de sistemas e do tráfego de informações, para garantir o sigilo e a Integridade das informações de Clientes mantidas sob sua guarda. Para manter a Segurança Cibernética, o Participante deve, no mínimo, manter controles para:

122.1.1. controle de acessos aos sistemas internos e disponibilizados aos Clientes (incluindo acessos remotos aos sistemas internos do Participante), incluindo um fator de autenticação para identificação dos clientes nas plataformas de negociação quando identificado acesso ou operação em cenários de risco.

Mecanismo de Prevenção a Fraude e Segurança Cibernética | Capítulo 12 – Segurança das Informações

Audiência Pública Restrita

122.1.4. manutenções e atualizações técnicas e de segurança da informação dos sistemas para atender as necessidades do negócio;

122.2.1. Monitoramento contínuo da segurança da rede do Participante, incluindo: (a) procedimentos para detecção de roubo de credenciais de clientes (usuários) para acesso aos sistemas do Participante e (b) processo de aprovação das regras pela área responsável antes da implantação e revisão periódica das regras implantadas;

122.2.3. procedimentos que permitam a detecção e resposta a um ataque realizado em dispositivos conectados às redes utilizadas pelo Participante;

Exclusão dos Itens:
123 – Parâmetros Mínimos de Senhas de Rede e Sistemas Internos
124 – Parâmetros Mínimos de Senhas de Clientes nos Canais de Relacionamento Eletrônico
128 – Ferramentas de Segurança de Redes

Mecanismo de Prevenção a Fraude e Segurança Cibernética | Capítulo 12 – Segurança das Informações

Audiência Pública Restrita

Atualização Item 125 - Os sistemas eletrônicos de negociação, de registro de Ordens, de cadastro, de gestão de risco, de custódia, de liquidação e gerenciamento de Perfil de Investimento dos Clientes (suitability) devem conter Trilhas de Auditoria suficientes para assegurar o rastreamento de eventos, incluindo:

125.3. identificação do evento, contendo a informação incluída, alterada ou excluída. Para os sistemas eletrônicos de cadastro fornecidos e gerenciados pelo Participante ou por terceiro por ele contratado, os eventos das Trilhas de Auditoria devem ser suficientes para assegurar a rastreabilidade da origem do cadastro (IP do usuário e/ou de outros que permitam identificação da origem);

Mecanismo de Prevenção a Fraude e Segurança Cibernética | Glossário

Inclusão - Cenários de Risco: Tentativa de acesso fora do padrão, inserção de ordem fora do padrão do cliente e identificação de origem de ordens em operações com características atípicas.

Teste de Estresse de Liquidez | Capítulo 6 – Gerenciar Risco

Novo Item

Inclusão Item 87 - O Participante deve desenvolver e documentar teste de estresse de liquidez, o qual deve ser atualizado diariamente, de acordo com a metodologia de teste de estresse divulgada pela B3 ou metodologia própria.

87. 1 Caso o participante opte por metodologia própria, esta deverá cobrir os cenários mínimos descritos na Nota Técnica e ser previamente encaminhada para avaliação da B3.

[B]³ **Tecnologia** | Capítulo 14 – Monitoramento e Operação da Infraestrutura de TI

Audiência Pública Restrita

Atualização Item 134 - O Participante deve monitorar a execução das rotinas de cópias de dados e voz, monitorar a execução, incluindo procedimentos de registro e de solução de erros, e testar a Integridade das informações armazenadas, que permitam a recuperação e garantam a disponibilidade das informações.

Atualização Item 136 - O Participante, a fim de garantir a integridade, a segurança e a disponibilidade de seus sistemas críticos, deve monitorar preventivamente a capacidade, o desempenho, a disponibilidade e o serviço da infraestrutura que suporta seus sistemas de rede e dos canais de comunicação, dos sistemas, dos servidores e do banco de dados, de forma a manter a continuidade e o bom funcionamento dos negócios.

Exclusão do Item:
133 – Documentos contendo os Procedimentos de *Backup*

Itens Excluídos

- **Capítulo 12 – Segurança das Informações**

Exclusão Itens:
123 – Parâmetros Mínimos de Senhas de Rede e Sistemas Internos
124 – Parâmetros Mínimos de Senhas de Clientes nos Canais de Relacionamento Eletrônico
128 – Ferramentas de Segurança de Redes

- **Capítulo 14 – Monitoramento e Operação da Infraestrutura de TI**

Exclusão Item 133 – Documentos contendo os Procedimentos de *Backup*

- **Capítulo 15 – Gerenciamento de Mudanças**

Exclusão Item 141 – Manutenções e Atualizações Técnicas e de Segurança

Itens Excluídos

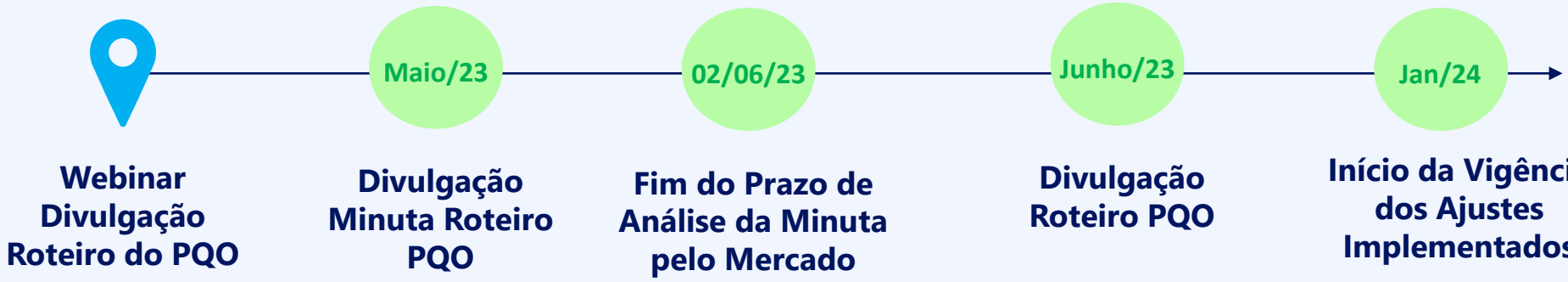
- **Capítulo 16 – Suporte à Infraestrutura**

Exclusão Itens:
146 – Homologação de Software e Licença de Uso
147 – Software Antivírus

- **Glossário**

Trilhas de Auditoria
Item excluído: inclusão e alteração de assessor

Plano de Implementação



Q&A

Obrigado!