18 de janeiro de 2024

CE 04/2024-BSM

N O R M A D E S U P E R V I S Ã O

Participantes dos Mercados da B3 – Listado

Ref.: **Norma de Supervisão sobre Segurança da Informação**

A BSM Supervisão de Mercados ("BSM"), no exercício de suas funções, emite a presente norma de supervisão ("Norma de Supervisão") para tratar dos procedimentos de supervisão da BSM sobre segurança da informação, considerando a regulamentação vigente da Comissão de Valores Mobiliários ("CVM") e as normas emitidas pela B3 S.A. – Brasil, Bolsa, Balcão ("B3").

Os termos definidos estão de acordo com o Glossário da BSM[1] ou são definidos na presente Norma de Supervisão.

A Norma de Supervisão está dividida em 6 (seis) seções: (I) Deveres do Participante; (II) Treinamento de segurança da informação e segurança cibernética; (III) Ameaças e vulnerabilidades no ambiente tecnológico; (IV) Atualizações técnicas de segurança; (V) Atuação da BSM; e (VI) *Enforcement*.

[1] Disponível em: https://www.bsmsupervisao.com.br/legislacao-e-regulamentacao/leis-normas-e-regras.

I. Deveres do Participante

1.1 É dever do Participante, conforme previsto na Resolução CVM nº 35/2021 ("RCVM 35"), garantir a integridade, a segurança e a disponibilidade dos seus sistemas críticos, desenvolvendo e implementando regras, procedimentos e controles internos adequados para garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade de dados e informações sensíveis.

1.2 A RCVM 35 estabelece a obrigatoriedade do Participante manter política de segurança da informação e segurança cibernética ("Política de Segurança"), a qual deve prever a periodicidade com que os funcionários, prepostos e prestadores de serviços devem ser treinados, os procedimentos de segurança da informação e os programas de segurança cibernética.

1.3 Nesse sentido, o Participante deve oferecer treinamento para capacitação dos funcionários, prepostos e prestadores de serviços, quanto as regras estabelecidas pela instituição ("Treinamento de Segurança da Informação e Segurança Cibernética" e/ou "Treinamento").

1.4 O Participante deve dispor de iniciativas que objetivem o monitoramento de ameaças e vulnerabilidades internas e externas, assim como a manutenção e atualizações técnicas e de segurança da sua infraestrutura.

1.5 A Política de Segurança, as informações referentes aos Treinamentos e as respectivas documentações previstas nesta Norma de Supervisão devem ser mantidas pelo Participante nos termos exigidos pela regulação.

II. Treinamento de Segurança da Informação e Segurança Cibernética

2.1. O Participante deve implementar programa de conscientização que contemple a realização de Treinamento de Segurança da Informação e Segurança Cibernética dos funcionários, prepostos e prestadores de serviço, com frequência mínima anual.

2.2 O Treinamento deve conter medidas de aderência como, por exemplo: provas, testes de *phishing* e planos de ação para conscientização daqueles que não atingirem o resultado mínimo esperado.

2.3 A forma de medir a aderência, o resultado mínimo esperado após o Treinamento e o plano de ação de conscientização devem constar da Política de Segurança do Participante, assim como a periodicidade desses Treinamentos.

2.4 O Treinamento deve ser aplicado, no mínimo, aos funcionários, prepostos e prestadores de serviço que tenham acesso a dados e informações sensíveis[2].

2.5 Além disso, o Participante pode reavaliar a aplicação do Treinamento quando concluir, de forma fundamentada, que os prestadores de serviço com acesso aos dados e informações sensíveis apresentam procedimentos de segurança da informação e de treinamento adequados e compatíveis com suas políticas. O fundamento para não aplicação do Treinamento deve ser mantido pelo Participante nos termos exigidos pela regulação.

[2] Dados ou informações sensíveis são aqueles assim classificado pelo Participante, observado o disposto no parágrafo único do artigo 42 da RCVM 35.

III. Ameaças e Vulnerabilidades no Ambiente Tecnológico

3.1 O Participante deve realizar, no mínimo anualmente, avaliações de ameaças e vulnerabilidades internas e externas da rede de computadores e infraestruturas dos sistemas que atendem as necessidades do negócio, incluindo o registro das ações tomadas, sendo que a documentação deve contemplar no mínimo:

a) a infraestrutura objeto de avaliação, com a identificação, avaliação e prevenção dos riscos internos e externos e a adoção de uma estrutura efetiva de controle e resposta para riscos cibernéticos, assegurando a implementação de práticas gerais e sólidas para gestão de riscos; e

b) o tratamento, as causas e os impactos das ameaças internas e externas detectadas.

IV. Atualizações Técnicas e de Segurança

4.1 O Participante deve adotar procedimentos para atualização de segurança dos sistemas operacionais, bem como para realização de testes em ambiente de homologação para verificação da compatibilidade do sistema antes da atualização no ambiente de produção.

4.2 Os procedimentos devem conter um prazo máximo para atualização após a divulgação do fornecedor. Esse prazo não deve ser maior que 90 (noventa) dias para atualizações consideradas críticas.

4.3. O Participante deve realizar a verificação de compatibilidade das atualizações de segurança em todas as versões de sistemas operacionais utilizadas pelo Participante em produção.

4.4. O Participante deve adotar processos de atualização de "patches[3]" de segurança. Caso o Participante entenda que a atualização não é aplicável devido às características do seu ambiente, o Participante deve formalizar as justificativas que o levaram a optar pela não instalação, em tempo hábil, após a data de divulgação da atualização.

V. Atuação da BSM

5.1 A supervisão e fiscalização da BSM em relação aos deveres acima expostos ocorre por meio de suas auditorias e supervisões contínuas, conforme testes definidos no Roteiro de Testes.

5.2 Durante a supervisão e fiscalização do Participante sobre segurança da informação, a BSM verifica o cumprimento das seguintes situações:

a) A implementação do Treinamento de Segurança da Informação e Segurança Cibernética abrangendo no mínimo o disposto nesta Norma de Supervisão e na regulação em vigor;

b) Os mecanismos de avaliação das ameaças e vulnerabilidades internas e externas da rede e das infraestruturas dos sistemas que atendem as necessidades do negócio, contendo no mínimo o disposto nesta Norma de Supervisão e na regulação em vigor; e

c) Os procedimentos para as atualizações técnicas e de segurança do Participante.

5.3 Sem prejuízo da realização das auditorias para avaliação do cumprimento da regulação e da presente Norma de Supervisão, a BSM poderá exigir declaração

[3] Trata-se de atualizações lançadas pelo fornecedor para a correção de pontos de segurança ou qualquer outro item dentro do sistema que vá garantir o melhor funcionamento.

do Diretor Responsável pelo Mercado, do Diretor responsável pelo cumprimento da RCVM 35 e do Diretor responsável pela supervisão dos procedimentos e controles internos do Participante, nos termos da referida norma, atestando o cumprimento das obrigações sobre segurança da informação, além do envio de evidências em relação ao Treinamento, histórico de atualização de segurança dos sistemas operacionais ocorridos durante determinado período e da realização de avaliações de ameaças e vulnerabilidades internas e externas da rede de computadores e infraestruturas dos sistemas que atendem as necessidades do negócio, com o envio de registros das ações tomadas.

VI. *Enforcement*

6.1 Os deveres indicados na regulação aplicável e na presente Norma de Supervisão, uma vez não atendidos adequadamente e tempestivamente pelos Participantes, serão considerados como agravantes para a aplicação de medidas de *Enforcement* estabelecidas no Regulamento Processual da BSM.

6.2 A presente Norma de Supervisão produzirá efeitos a partir de 1.2.2024.

Esclarecimentos adicionais poderão ser obtidos junto à Superintendência de Auditoria pelo e-mail bsm@bsmsupervisao.com.br ou telefone (11) 2565-6200, opção 3.

André Eduardo Demarco
Diretor de Autorregulação