18 de janeiro de 2024

CE 03/2024-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 no âmbito da Segregação de Funções**

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 referentes a segurança da informação no âmbito da segregação de funções, considerando a regulação 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) Segregação Lógica e Controle de Administração de Acessos; (III) Matriz de Segregação de Funções no Âmbito da Segregação Lógica; (IV) Segregação Física; (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. Para tanto, o Participante deve estabelecer regras, procedimentos e controles internos que sejam aptos a prevenir que os interesses dos clientes sejam prejudicados em decorrência de conflitos de interesse de funcionários, terceiros e prepostos.

1.3. As referidas regras, procedimentos e controles internos, no âmbito da segregação de funções, devem contemplar: (i) a proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso ou destruição não autorizados, vazamento ou adulteração; (ii) a concessão e administração de acessos individualizados a sistemas, bases de dados e redes; e (iii) a segregação de dados e controle de acesso, de forma a prevenir o risco de acesso não autorizado, de adulteração ou de mau uso das informações.

1.4. A documentação e evidências referentes ao cumprimento dos deveres previstos nesta Norma de Supervisão devem ser mantidas pelo Participante nos termos exigidos pela regulação.

II. Segregação Lógica e Controle de Administração de Acessos

2.1. Para assegurar a Segregação Lógica, o Participante deve dispor de controle de concessão de acessos definido de forma prévia.

2.2. O processo de concessão de acessos deve abranger toda a organização do Participante, em todos os níveis hierárquicos e em todas as funções. O processo deve conter, no mínimo, as seguintes características:

a) Ser usuário individual e não compartilhado;

b) Estar protegido por senha ou por método com segurança equivalente;

c) Ser concedido de forma a evitar o conflito de interesses e acessos em desacordo com a função desempenhada. Para isso, o Participante deve definir, previamente à concessão dos acessos, as atividades pertinentes à função exercida e as atividades que, acumuladas e executadas pelo mesmo profissional nos sistemas, possam gerar o conflito de interesses, as quais devem ser passíveis de verificação;

d) Exigir a certificação necessária para o despenho da função, conforme regra da B3;

e) Avaliar a qualificação técnica do usuário em relação ao acesso concedido;

f) Ser aprovado pelo proprietário da informação, ou seja, aquele formalmente designado como responsável pela autorização de acesso às informações; e

g) Ser concedido somente a profissionais que atuam para o Participante.

2.3. Conforme regra vigente na data de publicação da presente Norma de Supervisão sobre exigência de certificação[2], aos profissionais que ainda não possuam certificação e ingressarem no Participante a partir de 1.1.2024 é facultado período de experiência de 120 (cento e vinte) dias corridos a contar de seu registro no Sincad para obtenção da Certificação PQO. Após o período de 120 (cento e

[2] Ofício-Circular 2014/2023-PRE da B3, publicado em 21.12.2023.

vinte) dias, o Participante deve manter a comprovação da certificação desse profissional.

2.4. Durante o período de 120 (cento e vinte) dias acima disposto, o Diretor de Relações com o Mercado do Participante ao qual o profissional está vinculado será responsável pelos atos praticados por este profissional, sem prejuízo da responsabilidade individual do profissional.

2.5. O Participante deve administrar as concessões, alterações e exclusões dos acessos e manter o histórico devidamente arquivado, conforme regulação vigente.

2.6. No caso de existência de usuários não nominais ou usuários genéricos com acesso ativo, o Participante deve conter o histórico que demonstre a formalização e ciência da atribuição de responsabilidade pelo usuário, conforme procedimento previamente definido pelo Participante.

2.7. Para os funcionários, terceiros e prepostos desligados, o Participante deve adotar práticas que visem a mitigação de riscos, de forma que o processo de retirada dos acessos ocorra o mais rápido possível, sendo que após o desligamento desse profissional não deverão constar acessos aos sistemas do Participante por meio deste usuário.

III. Matriz de Segregação de Funções no âmbito da Segregação Lógica

3.1. O Participante deve manter, de forma prévia à concessão do acesso, uma Matriz de Segregação de Funções (“Matriz”) com as atividades que, quando cumuladas e executadas pelo mesmo profissional, possam gerar conflitos de interesses, definindo quais são os acessos permitidos de acordo com a função exercida por cada funcionário, terceiro ou preposto. O Anexo I a presente Norma

de Supervisão traz exemplos de Matrizes, as quais deverão ser adaptadas, se necessário, para o caso concreto do Participante.

3.2. O Participante poderá manter sistema equivalente à Matriz, desde que cumpra a mesma função e que seja passível de verificação.

3.3. A Matriz deve conter todas as atividades críticas pertinentes a cada função/área exercida, contendo no mínimo:

a) Inclusão, alteração e cancelamento de ofertas e ordens de clientes;

b) Inclusão, alocação, alteração e exclusão do registro de ordens de clientes (pós negociação);

c) Inclusão e manutenção de valores financeiros lançados na conta de registro (conta gráfica) dos clientes;

d) Transferência de custódia de clientes;

e) Inclusão e manutenção de dados cadastrais de clientes;

f) Inclusão e alteração de Perfil de Investimento de clientes/questionário;

g) Inclusão e alteração de parâmetros que compõem os limites operacionais dos clientes (risco pós negociação);

h) Inclusão e alteração de limites operacionais de clientes (risco pré negociação);

i) Atividades administrativas de sistemas aplicativos e de negociação (alteração de parâmetros, gestão e usuários, bloqueio e desbloqueio de senhas);

j) Correlação de todas as áreas mencionadas na Matriz com as respectivas nomenclaturas utilizadas pela área de gestão de pessoas ou área equivalente;

k) As atividades que, acumuladas e executadas pelo mesmo profissional nos sistemas, possam gerar conflitos de interesses, contendo no mínimo, os seguintes conflitos: (i) transferência de custódia de clientes por profissionais que desempenhem atividades de operações; (ii) inclusão e alteração de limites pré-operacionais de clientes por profissionais que desempenhem atividades de operações; e (iii) atualização de dados bancários por profissional de liquidação; e

l) Os procedimentos de exceção à Matriz, com a etapa de inclusão de uma justificativa para aprovação do acesso concedido em caráter excepcional.

3.4. Cabe ao Participante a definição do modelo de Matriz que melhor se adeque ao seu modelo de negócio. O modelo empregado na elaboração da Matriz deve ser suscetível de validação, com informações que sejam necessárias e suficientes para supervisão da BSM.

3.5. As permissões de acesso determinadas na Matriz devem ser revisadas, no mínimo, anualmente, evitando a concessão de acessos indevidos e divergentes da regulação em vigor.

3.6. O Diretor de Controles Internos deve emitir relatório anual de avaliação de controles internos, abrangendo, entre outros pontos, avaliação da segregação lógica das funções desempenhadas pelos funcionários, terceiros e prepostos, incluindo o acesso aos dados e informações sensíveis, de forma que não seja materializado o conflito de interesses.

IV. Segregação Física

4.1. O Participante, considerando o volume, natureza e complexidade de suas operações e estrutura, deve adotar métodos para garantir a segregação física de suas instalações, com o objetivo de mitigar as situações que propiciem conflitos de interesses e acessos em desacordo com as funções desempenhadas.

4.2. Os métodos devem permitir a criação e manutenção de uma estrutura segura e suficiente para o cumprimento da presente Norma de Supervisão, de forma a definir, restringir, fiscalizar e monitorar quem são os profissionais com acesso as informações e instalações sensíveis.

4.3. Nesse sentido, não basta a aplicação de processos, sendo também necessária a comprovação de que as medidas impostas são efetivas, por meio da adoção de procedimentos operacionais, com objetivo de:

a) Mitigar a ocorrência de irregularidades, conforme disposto na regulação vigente;

b) Promover a segregação funcional das áreas responsáveis pela Administração de Recursos de Terceiros das demais áreas que possam gerar potenciais conflitos de interesses, de forma a minimizar adequadamente tais conflitos;

c) Garantir a segregação física da mesa de operações das demais mesas de operações pertencentes a outras instituições do mesmo grupo e/ou conglomerado financeiro, exceto nos casos em que o Participante somente opere para essas instituições ou em que, comprovadamente, a partir de motivação do Participante, não houver conflito de interesses;

d) Garantir a segregação física das atividades de gestão de carteiras de valores mobiliários de terceiros, incluindo clubes de investimentos, das demais atividades de execução de ordens; e

e) Vedar a presença de cliente, em qualquer hipótese, no ambiente da mesa de operações.

4.4. O Participante deve aplicar medidas de conscientização e informação aos funcionários, terceiros e prepostos sobre as violações ou possíveis violações das disposições referentes à segregação física.

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 segregação de funções, a BSM verifica o cumprimento das seguintes situações:

a) Existência e suficiência da Matriz de segregação de funções, contemplando, no mínimo, todas as atividades críticas listadas nesta Norma de Supervisão, todos os sistemas e todas as áreas relacionadas a elas;

b) Avaliação das áreas e/ou funções da Matriz, verificando a relação direta ou equivalência com as áreas dos profissionais estabelecidas pelo departamento de Recursos Humanos, realizando o cruzamento da lista de usuários com a relação de profissionais vinculados;

c) Verificação da Matriz com a previsão dos conflitos mencionados no item 3.2 da presente Norma de Supervisão;

d) Caso a Matriz permita os conflitos mencionados acima, análise da existência de controles compensatórios para monitorar os usuários com esses acessos conflitantes;

e) Avaliação dos acessos concedidos aos sistemas e se estão de acordo com a Matriz de segregação de funções;

f) Em caso de existência de alguma exceção, avaliação dos acessos e se foram previamente aprovados e indicados na documentação; e

g) Medidas aplicadas para garantia da segregação física das áreas com potenciais conflitos de interesses.

5.3. Sem prejuízo da realização das auditorias para avaliação do cumprimento da regulação e da presente Norma de Supervisão conforme acima descrito, a BSM poderá exigir declaração 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 segregação de funções, além do envio de evidências da existência da Matriz, da segregação lógica e física e do tratamento dos potenciais conflitos de interesses.

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

ANEXO I – Matriz de Segregação de Funções

Segregação de Funções: Exemplos de Matrizes de Segregação de Funções

Modelo I - Áreas / Função x Atividades Permitidas

1. Nesse modelo são elencadas todas as atividades consideradas críticas e todas as áreas/funções dos funcionários, terceiros e prepostos que executam ou visualizam dados relacionados a essas atividades.

Áreas / Atividades	BACKOFFICE	CADASTRO	MESA DE OPERAÇÕES	RISCO	TECNOLOGIA DA INFORMAÇÃO
ADMINISTRAÇÃO	-	-	-	-	EDIÇÃO
ALTERAÇÃO DE CORRETAGEM	EDIÇÃO	EDIÇÃO	CONSULTA	-	-
CADASTRO DE CLIENTE	EDIÇÃO	EDIÇÃO	CONSULTA	CONSULTA	-
CADASTRO LIMITE PRÉ	-	-	-	EDIÇÃO	-
GERENCIAMENTO DE USUÁRIOS	-	-	-	-	EDIÇÃO
OPERAÇÃO	-	-	EDIÇÃO	-	-
TRANSFERÊNCIA DE CUSTÓDIA	EDIÇÃO	-	-	-	-

2. É recomendado que o Participante mantenha um documento complementar com a indicação dos perfis utilizados para execução de cada atividade crítica em cada sistema, conforme exemplo abaixo.

Sistema de negociação		
Perfil	**Área**	**Transações críticas (atividades)**
Operação	Mesa de Operações	Inclusão, alteração e cancelamento de ofertas e ordens de clientes
Administrador	TI	Atividades administrativas de sistemas (alteração de parâmetros, gestão de usuários, bloqueio e desbloqueio de senhas)
Limites e Cancelamento de ofertas	Risco	Inclusão e alteração de parâmetros que compõem os limites operacionais dos clientes, inclusão e alteração de limites operacionais de clientes, e cancelamento de ofertas e ordens de clientes
Sistema de Cadastro		
Perfil	**Área**	**Transações críticas (atividades)**
Alterações cadastrais	Cadastro e *Back Office*	Inclusão e manutenção de dados cadastrais de clientes

Sistema de negociação		
Perfil	**Área**	**Transações críticas (atividades)**
Administrador	TI	Atividades administrativas de sistemas (alteração de parâmetros, gestão de usuários, bloqueio e desbloqueio de senhas)
Consulta	*Compliance,* Risco e Mesa de Operações	Consulta de dados cadastrais de clientes

3. No mínimo, todas as atividades críticas, conflitos mínimos e áreas devem estar mapeadas na Matriz e de acordo com as áreas definidas na área de Recursos Humanos.

Modelo II - Áreas / Função x Sistemas / Perfis Permitidos

Sistemas / Áreas	CADASTRO	BACKOFFICE	MESA DE OPERAÇÕES	RISCO	TECNOLOGIA DA INFORMAÇÃO
Sistema de Backoffice	Perfil: CADASTRO	Perfil: BACKOFFICE	Perfil: CONSULTA	Perfil: CONSULTA	Perfil: ADMINISTRADOR
Sistema de Cadastro de Cliente	Perfil: CADASTRO	-	Perfil: CONSULTA	Perfil: CONSULTA	Perfil: ADMINISTRADOR
Sistema de Custódia	-	Perfil: BACKOFFICE	-	-	Perfil: ADMINISTRADOR
Sistema de Negociação	-	-	Perfil: OPERAÇÃO	Perfil: RISCOS	Perfil: ADMINISTRADOR
Sistema de Risco Pré	-	-	-	Perfil: RISCOS	Perfil: ADMINISTRADOR

Modelo III - Atividades que acumuladas podem gerar conflitos de interesse

Funções	Cadastro de Cliente	Inclusão, alteração e cancelamento de ofertas e ordens de clientes	Inclusão e alteração de Perfil de Investimentos de clientes	Transferência de custódia de clientes	Atividades administrativas de sistemas
Inclusão e manutenção de dados cadastrais de clientes	-	Consulta	Consulta	Conflito	Conflito
Inclusão, alteração e cancelamento de ofertas e ordens de clientes	Consulta	-	Conflito	Conflito	Conflito
Inclusão e alteração de Perfil de Investimentos de clientes	Consulta	Conflito	-	Consulta	Conflito
Transferência de custódia de clientes	Conflito	Conflito	Consulta	-	Conflito
Atividades administrativas de sistemas	Conflito	Conflito	Conflito	Conflito	-

a) Esse modelo pode ser um complemento aos dois modelos anteriores e não é suficiente de forma isolada, visto que, além dos conflitos mínimos, a presente Norma de Supervisão prevê que a concessão do acesso deve ser realizada de forma a evitar os acessos em desacordo com a função desempenhada.

b) Todas as atividades críticas e conflitos mínimos devem estar mapeados na Matriz.