

**COMISSÃO DE VALORES MOBILIÁRIOS**

Rua Sete de Setembro, 111/2-5º e 23-34º Andares, Centro, Rio de Janeiro/RJ – CEP: 20050-901 – Brasil - Tel.: (21) 3554-8686

Rua Cincinato Braga, 340/2º, 3º e 4º Andares, Bela Vista, São Paulo/ SP – CEP: 01333-010 – Brasil - Tel.: (11) 2146-2000

SCN Q.02 – Bl. A – Ed. Corporate Financial Center, S.404/4º Andar, Brasília/DF – CEP: 70712-900 – Brasil -Tel.: (61) 3327-2030/2031

www.cvm.gov.br

Ofício-Circular nº 5/2020-CVM/SMI

Rio de Janeiro, 04 de agosto de 2020.

Aos

Diretores responsáveis pela Instrução CVM nº 505/11 junto aos Intermediários

Assunto: **I - Prazos de comunicação à SMI:**

a) Acionamento de Plano de Continuidade de Negócios (PCN);

b) Incidentes Relevantes em Sistemas Críticos;

c) Incidentes Relevantes de Segurança Cibernética.

II - Abrangência da vedação à aplicação de recursos de clientes.

Senhores Diretores,

Este Ofício-Circular tem como objetivo trazer orientações para os intermediários sobre dois assuntos que serão objeto da Instrução CVM nº 505/11, a partir das alterações introduzidas pela Instrução CVM 612/19, em vigor a partir de 01/09/2020:

(I) prazos de comunicação à SMI sobre situações relacionadas a PCN, Sistemas Críticos e Segurança Cibernética; e

(II) Abrangência da vedação à aplicação de recursos de clientes.

I – INTRODUÇÃO

1. A Instrução CVM nº 612/19, editada em 21/8/2019 e que entra em vigor em 1/9/2020, trouxe exigências relacionadas à tecnologia da informação, alterando e inovando dispositivos da atual Instrução CVM nº 505/11, norma da CVM sobre controles internos.

PRAZOS DE COMUNICAÇÃO À SMI

Plano de Continuidade de Negócios (PCN)

2. Com o advento da Instrução CVM nº 612/19, os intermediários deverão implementar plano de continuidade de negócios (PCN) que estabeleça procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos de negócio, bem como ações de comunicação internas e externas necessárias e os casos em que a comunicação deve se estender aos clientes (art. 35-A, inciso II, da Instrução CVM nº 612/19).

3. Dentre os processos considerados críticos, o PCN deve abranger os processos de recepção e execução de ordens e de conciliação e atualização das posições de seus clientes, com o objetivo de preservar o atendimento aos clientes (art. 35-A, § 1º, da Instrução CVM nº 612/19).

4. Na ocorrência de um evento que provoque o acionamento do PCN, os órgãos de administração e a SMI deverão ser comunicados tempestivamente, nos termos do art. 35-A, § 4º, da Instrução CVM nº 612/19.

5. E, conforme estipulado pelo § 5º do mencionado artigo, a comunicação deve apresentar:

I - causas do acionamento do plano de continuidade de negócios, indicando os processos críticos afetados;

II - medidas já adotadas pelo intermediário ou as que pretende adotar;

III - tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e

IV - qualquer outra informação considerada importante.

Sistemas Críticos

6. Definido no 'caput' do art. 35-B da Instrução CVM nº 612/19, sistemas críticos são todos computadores, redes e sistemas eletrônicos e tecnológicos que se vinculam aos processos críticos de negócios e que diretamente executam ou indiretamente fornecem suporte a funcionalidades cujo mau funcionamento ou indisponibilidade pode provocar impacto significativo nos negócios do intermediário.

7. Na ocorrência de incidentes relevantes que afetem seus sistemas críticos e tenham impacto significativo sobre os clientes, os órgãos de administração e a SMI deverão ser comunicados tempestivamente, nos termos do art. 35-C, § 1º, da Instrução CVM nº 612/19.

8. E, conforme estipulado pelo § 2º do mencionado artigo, a comunicação deve apresentar:

I - a descrição do incidente, indicando de que forma os clientes foram afetados;

II - avaliação sobre o número de clientes potencialmente afetados;

III - medidas já adotadas pelo intermediário ou as que pretende adotar;

IV - tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e

V - qualquer outra informação considerada importante.

Segurança Cibernética

9. O intermediário deve adotar política que contemple um programa de segurança cibernética, abrangendo, dentre outras, as medidas que devem ser adotadas para reduzir a vulnerabilidade da instituição

contra ataques cibernéticos, conforme prescreve o art. 35-H, inciso II, da Instrução CVM nº 612/19.

10. Na ocorrência de incidentes relevantes de segurança cibernética, os órgãos de administração e a SMI deverão ser comunicados tempestivamente, nos termos do 'caput' do art. 35-I.

11. E, conforme estipulado pelo § 1º do mencionado artigo, a comunicação deve apresentar:

I - a descrição do incidente, incluindo indicação do dado ou informação sensível afetada;

II - avaliação sobre o número de clientes potencialmente afetados;

III - medidas já adotadas pelo intermediário ou as que pretende adotar;

IV - tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e

V - qualquer outra informação considerada importante.

12. E ainda, nos termos do § 2º do mesmo artigo, o intermediário deve elaborar e enviar à SMI relatório final contendo no mínimo:

I - descrição do incidente e das medidas tomadas, informando o impacto gerado pelo incidente sobre a operação da instituição e seus reflexos sobre os dados dos clientes; e

II - os aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar a ocorrência de incidentes de segurança cibernética, se for o caso.

13. Por fim, agora nos termos do § 3º ainda do mesmo artigo, o intermediário deve manter à disposição da SMI cópia:

I - das comunicações realizadas com seus clientes, se houver; e

II - dos relatórios internos de investigação produzidos pelo intermediário ou por terceiros sobre a análise do incidente e as conclusões dos exames efetuados.

ABRANGÊNCIA DA VEDAÇÃO À APLICAÇÃO DE RECURSOS DE CLIENTES

14. Ainda, a Instrução CVM nº 612/19 trouxe, em seu art. 35, novas vedações à atuação do intermediário, dentre elas, a constante do inciso XI, que veda ao intermediário aplicar, na constituição e operação de sua carteira, recursos de clientes.

II – PRAZOS PARA OS INTERMEDIÁRIOS COMUNICAREM A SMI

PCN e Sistemas Críticos

15. Inicialmente, há de se destacar que sistemas críticos são todos computadores, redes e sistemas eletrônicos e tecnológicos que se vinculam aos processos críticos de negócios e que diretamente executam ou indiretamente fornecem suporte a funcionalidades cujo mau funcionamento ou indisponibilidade pode provocar impacto significativo nos negócios do intermediário.

16. E, dentre os processos considerados críticos, o PCN deve abranger os processos de recepção e execução de ordens e de conciliação e atualização das posições de seus clientes.

17. Nesse contexto, considera-se tempestiva a comunicação à SMI, seja na ocorrência de um evento que provoque o acionamento do PCN (art. 35-A, § 4º, da Instrução CVM nº 612/19), seja na ocorrência de incidentes relevantes que afetem seus sistemas críticos e tenham impacto significativo sobre os clientes (art. 35-C, § 1º, da Instrução CVM nº 612/19), o prazo de, respectivamente:

I - até 72 (setenta e duas horas), após o acionamento do PCN;

II - até 72 (setenta e duas horas), após a materialização do incidente.

Segurança Cibernética

18. Por sua vez, com relação à ocorrência de incidentes relevantes de segurança cibernética, há de se considerar que as ameaças cibernéticas evoluem rapidamente, tanto em volume quanto em sofisticação, pelo que se entende as dificuldades que cada intermediário enfrenta em face das múltiplas características dos ataques cibernéticos.

19. Inclusive, após a materialização confirmada do ataque cibernético, há de se supor que cada intermediário terá uma resposta diferenciada, muito em razão da complexidade em enfrentar o ataque cibernético caso a caso.

20. Por essas razões, a SMI entende que, no atual momento, não deve ser fixado um prazo para a comunicação de incidentes relevantes de segurança cibernética.

21. No entanto, uma vez o intermediário tendo confirmado a materialização do ataque cibernético, em toda a sua extensão, e estabelecido planos de ação para mitigá-lo, deverá comunicar de imediato à SMI, para atender ao art. 35-I, 'caput', da Instrução CVM nº 612/19.

III – ABRANGÊNCIA DA VEDAÇÃO À APLICAÇÃO DE RECURSOS DE CLIENTES

22. É certo que a Instrução CVM nº 612/19 introduziu a vedação do intermediário aplicar recursos de clientes em operações de sua carteira.

23. No entanto, há de se ressaltar que a Instrução é destinada aos intermediários do mercado de valores mobiliários, pelo que, a mencionada vedação abrange tão somente a aplicação de recursos de clientes em valores mobiliários, quando aplicada em nome da carteira do intermediário.

24. Apesar da vedação atingir tão somente aplicação em valores mobiliários, ainda assim, para fins do art. 30, 'caput' e parágrafo único, da atual Instrução CVM nº 505/11, deve haver o comando prévio do cliente para permitir ao intermediário aplicar seus recursos em outras aplicações que não em valores mobiliários.

IV – CONCLUSÃO

25. Destaque-se, mais uma vez, que a transparência no mercado de intermediação é requisito da Instrução CVM nº 505/11, refletida em seu art. 30, vedando ao intermediário privilegiar seus próprios interesses:

Art. 30. O intermediário deve exercer suas atividades com boa fé, diligência e lealdade em relação a seus clientes.

Parágrafo único. É vedado ao intermediário privilegiar seus próprios interesses ou de pessoas a ele vinculadas em detrimento dos interesses de clientes.

Atenciosamente,



Documento assinado eletronicamente por **Francisco José Bastos Santos, Superintendente**, em 04/08/2020, às 15:01, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.



A autenticidade do documento pode ser conferida no site https://sei.cvm.gov.br/conferir_autenticidade, informando o código verificador **1068365** e o código CRC **29B71BDA**.

*This document's authenticity can be verified by accessing https://sei.cvm.gov.br/conferir_autenticidade, and typing the "Código Verificador" **1068365** and the "Código CRC" **29B71BDA**.*

Referência: Processo nº 19957.005135/2019-17

Documento SEI nº 1068365