INSTRUCTIVO **OPERATIVO**

N° BNIO-2025-7

Protocolo de integración técnica para la implementación de nuevas tecnologías por parte de las sociedades comisionistas de Bolsa

Bogotá, mayo de 2025

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

BMC BOLSA MERCANTIL DE COLOMBIA

TABLA DE CONTENIDO

1. INTRODUCCIÓN

1.1. Propósito del documento y objetivos clave

El presente protocolo tiene como finalidad establecer un marco técnico y operativo para la integración de sistemas automatizados y/o ayudas tecnológicas de las Sociedades Comisionistas de Bolsa (en adelante "SCB") con las plataformas de la Bolsa mercantil de Colombia S.A. (en adelante "BMC" o "Bolsa") bajo principios de transparencia, trazabilidad, seguridad de la información y protección de la infraestructura, previniendo prácticas abusivas y protegiendo la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica suministrada por el Bolsa al mercado.

Su implementación responde a la necesidad de garantizar que el uso de herramientas automatizadas se realice en un entorno controlado, seguro y en estricto cumplimiento de las normativas aplicables, así como de la protección de la infraestructura tecnológica y sistemas de información de la Bolsa Mercantil de Colombia.

En ese sentido, se definen las condiciones y términos bajo los cuales las SCB y sus sistemas automatizados (incluidos robots de negociación, APIs, y otras herramientas tecnológicas) se integrarán y utilizarán la infraestructura de las plataformas de la BMC, bajo los siguientes objetivos clave:

- **Establecer requisitos técnicos** para la integración de sistemas automatizados y/o ayudas tecnológicas de las SCB con la infraestructura y sistemas de la BMC.

- **Definir criterios de evaluación y validación** para garantizar que los sistemas cumplen con los estándares de seguridad de la norma ISO/IEC 27001 y demás políticas establecidas en la BMC.

- **Regular el uso de estrategias automatizadas**, estableciendo restricciones sobre aquellas prácticas que puedan representar un riesgo para la estabilidad de la infraestructura y sistemas de información de la BMC.

- **Establecer** medidas que promuevan la identificación, prevención y mitigación de los riesgos y efectos no deseados relacionados con afectación a las plataformas tecnológicas de la BMC.

1.2. Alcance y aplicación

De conformidad con lo establecido en el artículo 1.6.7.2. de la Circular Única de Bolsa, este protocolo es de aplicación obligatoria para todas las SCB que pretenda interactuar con los sistemas de información de la BMC.

Los lineamientos contenidos en este documento abarcan el proceso de integración y validación de sistemas, la supervisión y monitoreo de las actividades realizadas por estos y la delimitación de las estrategias permitidas y prohibidas.

1.3. Definiciones clave

Para efectos de este protocolo, se establecen las siguientes definiciones que permitirán una comprensión uniforme de los términos empleados:

- **API:** es una interfaz de programación de aplicaciones.

- **API REST:** es una interfaz de programación de aplicaciones (API) que se ajusta a los principios de diseño del estilo arquitectónico de transferencia de estado representacional (REST). Las API REST proporcionan una forma flexible y ligera de integrar aplicaciones y conectar componentes en arquitecturas de microservicios.

- **Circuit breakers:** es un mecanismo de protección utilizado para detener temporalmente las negociaciones en el mercado en caso de un movimiento repentino e inusual en los precios de los activos. Esto se utiliza para evitar pérdidas masivas en caso de un colapso del mercado. El objetivo es frenar la volatilidad extrema, dar tiempo a los inversores y reguladores para analizar la situación y evitar que las pérdidas se acumulen.

- **Estándar:** es un conjunto de reglas, directrices o especificaciones que definen cómo deben implementarse o funcionar ciertos sistemas, tecnologías o procesos. Los estándares son establecidos para garantizar la compatibilidad, interoperabilidad, calidad y seguridad en diversas áreas de la tecnología.

- **Failover:** es la conmutación por error de un modo operativo de respaldo en el que un componente secundario asume las funciones de un componente del sistema cuando el componente principal deja de estar disponible ya sea por falla o por tiempo de inactividad programado. La conmutación por error es una parte integral de los sistemas de misión crítica.

- **FastAPI:** es un framework web moderno, rápido (de alto rendimiento), para construir APIs con Python basado en las anotaciones de tipos estándar de Python.

- **Front-running:** es una práctica ilegal de mercado que consiste en adelantarse a una operación de compra o venta de un activo en bolsa, que se sabe va a producirse en el corto plazo y que, a causa de su elevado volumen, va a afectar significativamente a su precio, beneficiándose el operador de ello para obtener beneficio a su costa.

- **High-Frequency Trading (HFT):** Estrategia de negociación algorítmica que implica la ejecución de un gran número de órdenes en fracciones de segundo con el propósito de obtener ventajas en los precios o velocidad de las posturas.

- **Lenguaje de programación:** es un conjunto de instrucciones que los programadores usan para escribir software. Los lenguajes de programación permiten crear aplicaciones, sitios web, videojuegos y más. Cada lenguaje tiene una sintaxis y reglas específicas que dictan cómo debe escribirse el código.

- **Plataforma de negociación:** Servicios tecnológicos proporcionados por la BMC que permite la ejecución de operaciones del mercado, ya sea de forma manual o automatizada.

- **Protocolo:** es un conjunto de reglas o convenciones que definen cómo deben comunicarse los sistemas o dispositivos entre sí. En informática, un protocolo asegura que los datos se envíen y reciban correctamente a través de una red o entre diferentes aplicaciones, estableciendo la forma y el orden en que la información debe ser intercambiada.

- **Robots:** Son maquinas programables que pueden realizar tareas de forma autónoma o semiautomática.

- **RPA (Robotic Process Automation) en español Automatización robótica de procesos:** Es una tecnología que automatiza tareas repetitivas y basadas en reglas, Los robots de software RPA se comunican con los sistemas para agilizar procesos y reducir la carga de trabajo de los humanos.

- **Sandbox o ambiente de pruebas:** Entorno controlado de pruebas donde se realizan verificaciones sobre la funcionalidad, eficiencia y seguridad de los sistemas automatizados antes de su implementación en un entorno productivo.

- **Scraping en español (raspado web):** Es una técnica que utiliza programas para extraer datos de forma automatizada de sitios web, almacenándonoslos en un formato estructurado para su uso posterior.

- **Scripts de automatización:** es un fragmento de código pequeño y específico que

puede ampliar el producto. Está compuesto por un punto de ejecución, variables con valores de enlace correspondientes y el código fuente.

- **Sistema automatizado de negociación:** Conjunto de herramientas informáticas, soluciones tecnológicas o automatizaciones y software diseñados para ejecutar operaciones de compra y venta en el escenario de negociación de la BMC de manera autónoma o semi-autónoma.

- **Spoofing:** es el nombre que se utiliza para referirse a los ataques por suplantación de identidad. La palabra viene del término inglés spoof, que significa suplantación

2. CUMPLIMIENTO DE REGLAS PARA EL USO DE ROBOTS, RPA, SCRAPING, U OTRAS TECNOLOGÍAS DE AUTOMATIZACIÓN

El desarrollo y uso de sistemas automatizados y ayudas tecnológicas están sujetos a un marco procedimental que busca garantizar la estabilidad del mercado, la transparencia en la ejecución de órdenes, y la estabilidad de la infraestructura de la BMC.

2.1. Buen uso de la plataforma

En línea con lo dispuesto en los artículos 1.6.7.1., 1.6.7.2. y 1.6.7.4. de la Circular Única de Bolsa, las SCB deberán validar que las soluciones y ayudas tecnológicas para el desarrollo de la gestión de sus Operadores en la rueda de negocios, así como de la transmisión de información hacia los sistemas administrados por la Bolsa, cumplan con los estándares técnicos, de seguridad, confiabilidad y trazabilidad establecidos en el presente protocolo.
En consecuencia, se presume que con el acceso a los sistemas administrados por la Bolsa, las SCB se comprometen a:

- No realizar **ataques de denegación de servicio (DoS)** o tipo DDoS que significa "Ataque de denegación de servicio distribuido (Distributed Denial-of-Service,)", ni actividades similares que puedan afectar la estabilidad de la plataforma o la calidad del servicio proporcionado a otros usuarios por parte de la BMC.

- No utilizar **scripts de automatización no aprobados, bots no verificados, herramientas de IA** y/o herramientas de **scraping de datos** para interactuar con las plataformas de la BMC, ni a implementar soluciones tecnológicas o automatizaciones o estrategias sin la debida presentación y/o autorización.

- No usar ningún robot o algoritmo automatizado, sin haber sido previamente revisado y validado por la BMC en un entorno de prueba (sandbox) provisto por cada sociedad, para asegurar el cumplimiento de las políticas de seguridad y operativas de los sistemas de la BMC.

- Operar dentro de los **límites operativos** establecidos por la plataforma y desarrollados en el numeral 2.4., como número de solicitudes, volumen de transacciones y frecuencia de órdenes.

2.2. Protección de Datos y Seguridad

Para la implementación de cualquier solución o ayuda tecnológica en los términos del artículo 1.6.7.2. de la Circular Única de Bolsa, las SCB deberán implementar medidas de seguridad adecuadas para proteger la confidencialidad y privacidad de los datos de sus clientes y prevenir accesos no autorizados o filtraciones de información, siguiendo la normatividad vigente de protección y privacidad de información y las demás que aplique.

En ese sentido, las SCB deberán realizar todas las comunicaciones a través redes debidamente cifradas, garantizando que realicen a través del protocolo HTTPS utilizando el cifrado TLS 1.2 o superiores para la transmisión de información y garantizando la protección de los datos de sus clientes y la integridad de las transacciones.

Los robots u otras tecnologías de automatización se deberán comunicar con los sistemas propios de la SCB solo a través de canales seguros (por ejemplo, HTTPS). Además, las SCB deberán verificar la integridad de las solicitudes utilizando firmas digitales o hashes para asegurar que las solicitudes no sean modificadas en tránsito.

Además, las SCB deberán verificar la integridad de las solicitudes utilizando firmas digitales o *hashes* para asegurar de que las solicitudes no sean modificadas en tránsito.

Las SCB deberán implementar otras medidas de seguridad como:

- Proporcionar claves para los algoritmos criptográficos asimétricos, como por ejemplo RSA SHA 512 o superiores.
- Proteger las cookies/objetos de sesión de autenticación para que no estén expuestas a ningún software cliente en el dispositivo del usuario.
- Emplear Secure DNS para evitar ataques de spoofing.
- No almacenar en control de código fuente, credenciales, llaves o contraseñas.

Para mitigar los riesgos asociados a la protección de datos y la ciberseguridad, las SCB que operan ayudas tecnológicas o automatizados, la BMC recomienda implementar controles estrictos en sus plataformas:

2.2.1. Autenticación reforzada y control de accesos

- Implementación de autenticación multifactor (MFA) para el acceso a cuentas.

- Restricción del acceso a la plataforma mediante verificación de dispositivos y control de geolocalización.

2.2.2. Cifrado de datos y privacidad de la información

- Uso de cifrado de extremo a extremo.

- Implementación de sistemas de anonimización y pseudonimización de datos personales.

2.2.3. Monitoreo y detección de amenazas en tiempo real

- Desarrollo de sistemas de detección de intrusos (IDS) y herramientas de análisis de comportamiento basadas en inteligencia artificial.

- Implementación de redes de vigilancia cibernética para detectar intentos de explotación de vulnerabilidades.

2.2.4. Planes de respuesta ante incidentes y auditorías de seguridad

- Desarrollo de protocolos de respuesta ante ciberataques, con procedimientos para mitigar impactos y restaurar operaciones.

- Ejecución de auditorías de seguridad y pruebas de penetración periódicas para evaluar la solidez de las defensas de la plataforma.

2.3. Proceso de integración y validación de sistemas automatizados

La integración de soluciones y ayudas tecnológicas con los sistemas de la BMC requiere un proceso riguroso de validación, con el objetivo de garantizar la compatibilidad técnica, la seguridad operativa y el cumplimiento normativo. Este proceso de integración y validación abarca pruebas técnicas, auditorías y análisis de desempeño; asegurando que los sistemas automatizados cumplan con los estándares establecidos antes de su implementación en entornos de producción.

Todo desarrollo o integración tecnológica deberá adherirse a un ciclo de vida seguro del Software (Secure Software Development Life Cycle – SDLC), el cual deberá contemplar, como mínimo, la ejecución de pruebas de seguridad, análisis de código fuente, implementación de controles conforme al estándar OWASP ASVS, y una revisión técnica integral previa a su paso al ambiente de producción así:

a) Compatibilidad con protocolos de comunicación y conectividad

- Se deben realizar pruebas de conectividad y latencia para evaluar el desempeño del sistema en tiempo real.

- Las SCB deben implementar mecanismos de redundancia y failover, garantizando la continuidad operativa en caso de fallos.

b) Seguridad informática y protección contra accesos no autorizados

- Se deben implementar mecanismos de autenticación robusta (autenticación multifactor, encriptación de datos, certificados digitales).
- El sistema debe contar con protocolos de prevención de ataques cibernéticos, incluyendo firewalls y detección de intrusos (IDS/IPS).
- Se requiere una evaluación de vulnerabilidades antes de la implementación en producción.

c) Mecanismos de control de errores y estabilidad operativa

- Se deben incluir filtros de validación de datos para evitar la ejecución de órdenes erróneas.
- El sistema debe contar con mecanismos de detección y corrección de fallos, asegurando que los errores no generen impactos sistémicos en el mercado.
- Se exige la implementación de sistemas de registro y auditoría, permitiendo la trazabilidad de todas las órdenes ejecutadas.

La BMC podrá requerir en cualquier momento la información relativa al cumplimiento de estos items.

2.4. Límites Operacionales y de Riesgo

Las SCB deberán abstenerse de ejecutar operaciones con tamaños excesivos que puedan alterar el mercado o generar riesgos no gestionados. La BMC se reserva el derecho de establecer límites de exposición por cuenta, por día, semana o mes.

Las SCB deberán limitar el número de órdenes por segundo que su robot u otra tecnología de automatización pueda realizar, con el fin de evitar sobrecargas en la infraestructura de la plataforma. Los límites de solicitudes estarán sujetos a la revisión de la BMC, de acuerdo con el tipo de operación. El límite inicial será de **5 transacciones por segundo**, el cual será implementado de manera provisional a partir de la fecha de inicio de la integración.

Este límite se establece con el entendimiento de que las condiciones de uso y la capacidad del sistema podrán variar a medida que se realicen pruebas adicionales y se evalúe el comportamiento real del sistema en el entorno de producción.

Por lo anterior, la BMC y las SCB realizarán las pruebas técnicas necesarias durante el periodo inicial de uso para calibrar el sistema y ajustar el límite de transacciones por segundo, según los resultados obtenidos y con el objetivo de garantizar un rendimiento óptimo y estable del sistema. Las SCB deberán proporcionar los datos y recursos necesarios para llevar a cabo dichas pruebas.

En función de los resultados de las pruebas y del uso real del sistema, se revisará el límite

de transacciones por segundo, y en caso de ser necesario, se modificará dicho límite por acuerdo mutuo, con base a las capacidades técnicas del sistema y a la infraestructura disponible en ese momento.

La BMC se reserva el derecho de ajustar el límite de transacciones por segundo en cualquier momento, en función de las pruebas realizadas y del comportamiento observado en el entorno de producción y de establecer tasas de cancelación máximas para evitar la manipulación de precios mediante la creación y eliminación masiva de órdenes.

La BMC puede exigir que se presenten informes detallados sobre las órdenes ejecutadas por los sistemas automatizados y/o ayudas tecnológicas, incluyendo información sobre los parámetros de decisión utilizados, las SCB deben proporcionar información sobre la velocidad de ejecución, tasas de cancelación de órdenes y latencia de las operaciones. Las SCB que usen ayudas tecnológicas, deben implementar sistemas de monitoreo en tiempo real que permitan detectar fallas o problemas en sus plataformas y deben contar con planes de emergencia en caso de fallas en sus soluciones tecnológicas o automatizaciones implementadas.

Las SCB deben contar con herramientas de supervisión continua para detectar anomalías en la ejecución de órdenes y la BMC puede exigir la implementación de interruptores de apagado de emergencia que permitan desactivar los soluciones tecnológicas o automatizaciones en caso de fallos.

2.5. Entorno de pruebas o sandbox

En cumplimiento del artículo 1.6.7.3. de la Circular Única de Bolsa, las SCB deberán diseñar, intercambiar y presentar ante la BMC los escenarios de casos de uso y diagramas de flujo de la solución a implementar o modificar y la interacción con los sistemas de la BMC. Lo anterior, con el fin de evitar cualquier ambigüedad en la comprensión del flujo de comunicación y establecer plan de integración que contemple pruebas funcionales y paso a producción.

Antes de ser implementados en un entorno de producción, las soluciones y ayudas tecnológicas, como por ejemplo, sistemas automatizados, deben ser sometidos a pruebas en un sandbox, donde se evalúa su desempeño en condiciones controladas, obedeciendo los siguiente parámetros:

- Antes de su implementación, las ayudas tecnológicas deben ser sometidos a escenarios de simulación para evaluar su desempeño bajo condiciones de mercado. Para el efecto, se deben replicar escenarios con diferentes niveles, a discrecionalidad de la BMC, evaluando la respuesta del sistema en distintas condiciones.

- Se requiere que las SCB cuenten con protocolos de gestión de emergencias en caso de fallas técnicas o pérdidas inesperadas.

- Se deben realizar pruebas de estrés sobre las soluciones tecnológicas presentadas para medir el impacto en la infraestructura de la BMC y las SCB

proporcionarán los datos y sus ambientes de pruebas.

- Se deben analizar los tiempos de ejecución y la interacción con la infraestructura de la BMC.

- Se deben realizar pruebas de carga y escalabilidad para verificar que los sistemas de la BMC puedan procesar grandes volúmenes de órdenes sin degradación del rendimiento. Para estas pruebas la SCB y la BMC convendrán las características de los ambientes de pruebas necesarios.

- En caso de requerir cambios en la técnica de automatización o parámetros de la herramienta, la SCB debe comunicar tal situación con 15 días calendario de anticipación a cualquier uso, y desde esa notificación correrá el tiempo correspondiente de 10 días hábiles para el análisis del ajuste, cambio de herramienta o cambio de parametrización en la herramienta de automatización.

Para la revisión de los parámetros previamente referidos, la SCB que desee implementar la solución o ayuda tecnológica debe solicitar el ambiente de pruebas por escrito a la Dirección de Producción e Infraestructura de la Vicepresidencia de Tecnología,

Si se desea hacer uso de robots u otras tecnologías de automatización, algoritmos o pruebas de carga y/o algún tipo de automatización de pruebas, solo se podrá hacer en el ambiente definido y habilitado por la BMC, previo a agendamiento de este ambiente.

Se aclara que el ambiente comentado en este numeral corresponde a la parte de los sistemas de información de la Bolsa, y las SCB deben proveer los ambientes de prueba correspondientes a las desarrollos por verificar.

2.6. Transparencia en reportes, auditoría y supervisión de Robots u otras tecnologías de automatización

En desarrollo del artículo 1.6.7.7. de la Circular Única de Bolsa, las soluciones tecnológicas o automatizaciones utilizados por las SCB para realizar operaciones en la plataforma podrán ser auditados y revisados periódicamente, en línea, o a demanda por la BMC para revisar el cumplimiento con las políticas de seguridad y operativas y con el fin de detectar comportamientos anómalos y asegurar el cumplimiento de las reglas de seguridad, operativas y de mercado.

Así mismo, estas auditorias podrán ser adelantadas sin previo aviso con el fin de velar con la transparencia de que lo que fue estipulado como herramienta y sus parámetros está siendo usada con los márgenes establecidos en el momento inicial de la inspección.

Cada SCB deberá proporcionar a la BMC:

- Los detalles completos sobre la lógica, estrategias y parámetros de los robots de negociación que se utilicen en la plataforma, permitiendo su auditoría y revisión periódica, estos deben tener la trazabilidad necesaria con el fin de que se pueda

realizar las acciones de supervisión.

- Los registros de las actividades de los robots y demás soluciones y ayudas tecnológicas implementadas, incluyendo el historial de órdenes, resultados y cualquier análisis de performance relacionado con las operaciones realizadas. Para el efecto, las soluciones y ayudas tecnológicas implementadas deben registrar cada transacción ejecutada, con trazabilidad total de los parámetros utilizados en la toma de decisiones, en caso de que dicha solución o ayuda contemple estas funcionalidades.

La información de trazabilidad debe garantizar su almacenamiento y consulta de la información por 5 años, con el fin de supervisar y ver el cumplimiento de las políticas y buenas prácticas de la plataforma y que no se viola ninguna norma de protección del mercado.

Las SCB deben mantener registros históricos de las versiones de las soluciones, incluyendo modificaciones y ajustes realizados.

La BMC está en la potestad de monitorear cualquier comportamiento inusual y alteración en los parámetros previamente conciliados.

3. ACTUALIZACIÓN Y REVISIÓN DEL PROTOCOLO

Este protocolo podrá ser actualizado por la BMC en cualquier momento. Las SCB serán notificadas de cualquier cambio y se comprometen a **acatar las nuevas condiciones** y ajustarse a las mismas.

Las SCB se comprometen a revisar y aceptar **nuevas versiones** de este protocolo de integración y uso, antes de proceder con la integración de cualquier nuevo sistema automatizado.

Las SCB aceptan que cualquier cambio o actualización será notificado con tiempo suficiente para permitir su revisión y adaptación.

BMC

BOLSA MERCANTIL DE COLOMBIA

@BolsaMercantil

@Bolsa Mercantil de Colombia Oficial