Aviso N° 489/14

LANZAMIENTO
ACCESO DIRECTO AL MERCADO

A partir de la fecha el MATba ha dispuesto el lanzamiento de la modalidad de "Acceso Directo al Mercado" (ADM), en el sistema de negociación MATba Trader, en virtud del cual los operadores podrán obtener autorización para ofrecer a sus comitentes esta nueva herramienta.

1. El Sistema de Acceso Directo al Mercado (ADM)

El ADM permite que los comitentes puedan ingresar, en forma controlada, ofertas en las ruedas del mercado, que operan mediante el sistema MATba Trader.

De esta manera, el sistema resultante además de robustez y eficiencia, ofrecería flexibilidad y un alto grado de conectividad entre el Mercado y sus diversos participantes

Con este desarrollo, los objetivos que se persiguen, entre otros, son:

- Facilitar el acceso de diversos participantes del mercado al ambiente de negociación electrónica, de forma de ampliar el poder de distribución y el grado de capilaridad de los productos ofrecidos por el MATba
- Posibilitar de automatizar el proceso de ejecución de órdenes, permitiendo mayores ganancias a escala, reducción de costos y mejor atención a los clientes.
- Posibilidad de generar nuevas líneas de negocios con la oportunidad de obtener mayores ingresos, mejorando de este modo la ecuación de rentabilidad.

2. Requisitos que deben cumplir los operadores para su autorización.

El operador que desee obtener autorización del MATba para utilizar este sistema deberá completar una solicitud al efecto en la cual brindará una explicación de los parámetros de control de riesgo *pre-trade* y *post-trade*.

En cuanto al control de riesgo *pre-trade*, deberá establecer los parámetros que tendrá en cuenta a los fines de:

1. Autorizar o suspender el acceso del cliente al sistema.
2. Definir los límites operacionales para el cliente, los cuáles serán verificados antes de procesar una orden dada.
3. Acompañar, en tiempo real, todas las ofertas ingresadas, pudiendo en cualquier momento cancelarlas, como así también los negocios cerrados.

En relación al sistema *post-trade*, deberá utilizar el Sistema de Valoración a Riesgo (SVR II) provisto por el MATba.

3. Responsabilidad del operador por las operaciones que realicen sus clientes.

El operador será totalmente responsable por el acceso de los comitentes a la Plataforma respecto de todas las órdenes ingresadas por éstos, así como las consecuentes operaciones generadas por dichas órdenes. Por ende, el operador podrá modificar las órdenes, cancelarlas y llegado el caso bloquear el acceso de los comitentes al sistema.

Teniendo en cuenta lo expresado, el operador tendrá a su cargo el cumplimiento de la totalidad de la normativa vigente (Ej.: Leyes, Decretos, Resoluciones de la CNV, UIF, Estatuto Social, Reglamento Social, Avisos y Circulares del MATba, etc.)

Asimismo, el MATba podrá suspender o cancelar definitivamente el acceso de uno o más comitentes, como así también la autorización concedida al operador.

4. Auditorías periódicas a los operadores

El MATba incluirá dentro de su Plan de Auditorias un punto específico, relativo a las autorizaciones de acceso vía ADM concedidas por el operador, a los fines de verificar el correcto seguimiento los parámetros *pre-trade* y *post-trade*, haciendo particular hincapié en el adecuado cumplimiento de las normas relativas a lavado de dinero.

5. Publicidad de la autorización concedidas por el MATba.

Las autorizaciones concedidas a los operadores serán publicadas en el sitio web institucional del MATba.

En anexo, se acompaña documento donde se explicitan las características y especificaciones técnicas.

El presente Aviso fue aprobado por el Directorio de la Comisión Nacional de Valores en su reunión del 17 de octubre de 2012.

Buenos Aires, 1° de julio de 2014.

Dra. Viviana I. Ferrari
Gerente General

ANEXO. Acceso Directo al Mercado - Características y especificaciones técnicas

1. CARACTERISTICAS TECNICAS

1.1. Autenticación

- La autenticación de los usuarios se realiza mediante Usuario/Password
- Las Passwords son encriptadas en el punto de entrada y son codificadas y almacenadas utilizando el algoritmo SHA-256.
- Las claves son configuradas utilizando el siguiente criterio de seguridad
    - Las claves deben contener 3 de los siguientes 4 tipos (Mayúsculas, minúsculas, números, signos de puntuación).
    - Las claves deben coincidir con un tamaño preestablecido (configurable).
    - Las claves expiran luego de un periodo de tiempo, y deben ser cambiadas por el usuario (configurable).
    - Las claves deben ser distintas a aquellas guardadas en el historial de claves (configurable).

1.2. Autorización de Acceso

Los usuarios son habilitados para acceder al sistema por Administradores. Los Administradores son configurados con roles definidos y se conectan al sistema a través de un canal SSL. Requieren de Usuario/Password, para acceder al sistema de administración.
Los derechos de acceso de los usuarios en el sistema, puede ser controlado. A cada usuario se le puede asignar un perfil de consulta o se le puede permitir negociar cada instrumento listado en el sistema.

1.3. Control de errores y control de secuencia

El protocolo de **PatSystems**, utiliza Id's únicos de mensaje, y utiliza el control de errores y secuenciamiento de la capa de transporte de la red.

1.4. Integridad

Este punto está cubierto por el uso de SSL. SSL previene de ataques *man-in-the-middle*, el cual es un ataque en el que un tercero adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado; Por lo tanto prevendrá que los mensajes sean modificados, dado que estos son encriptados. En el caso de que se requieran niveles adicionales de seguridad, puede implementarse VPN *tunneling* entre el cliente y el servidor.

1.5. Privacidad o confidencialidad

Las conexiones pueden hacerse/forzarse utilizando SSL. En el caso de que se requieran niveles adicionales de seguridad, puede implementarse VPN tunneling para la conectividad.

1.6. Irrefutabilidad o No Repudio

Cada vez que un usuario ingresa al sistema, se le asigna un Id de orden único. Este Id se asocia con cada orden puesta por el corredor a lo largo del sistema. De esta manera se puede hacer el seguimiento de una orden desde el momento en la que ingresó al mercado, hasta que la orden produce un cierre. Si la orden es modificada, cancelada o produce cierre, el sistema grabará quien ha ejecutado tales modificaciones.

1.7. No secuestro de Sesión (Non Hijacking)

SSL previene de ataques *man-in-the-middle*. También puede ser habilitada la autenticación del lado del cliente, donde cada cliente tiene un certificado único instalado en la máquina desde donde se conecta, para asegurar que sólo un usuario pueda conectarse desde una sola máquina.

1.8. No Reinyección o Repetición o Rejugabilidad (Non Replay)

Este punto está cubierto por el uso de SSL. Esto previene la inyección de código o ataques de reinyección cuando terceras partes graban los mensajes. Sumando a esto, los mensajes son auditados y solo son procesados aquellos que lleguen desde conexiones autenticadas seguras.

2. ESPECIFICACIONES TECNICAS

2.1. Conectividad

El acceso al sistema de trading electrónico se realiza a través de dos líneas WAN de 10 MB cada una (*Internet*). Los proveedores de las líneas son las empresas ***IPlan*** y ***Telmex***. Este tipo de conectividad, ofrece una alta disponibilidad y versatilidad respecto del lugar físico de conexión dado que, cada usuario podrá conectarse al sistema, desde donde tenga acceso WEB. Ambos servicios se ofrecen con los siguientes parámetros de calidad:

	Telmex	IPlan
Disponibilidad Mensual	99.5%	99.7%
Latencia Máxima	< 20 ms	<20ms
Perdida de Paquetes	< 0.1%	< 0.1%

2.2. Protección perimetral

El acceso en forma segura a Internet es provisto por un clúster de firewalls Cisco ASA 5520 (ASA-PME-01 y ASA-PME-02), conectándose a ambos proveedores de Internet por medio de dos switches redundantes Cisco Small Business SF 100D-08 para dar redundancia de enlace. Dicho clúster de firewalls trabaja en modo activo/pasivo, de manera que, en caso de que el firewall principal falle, se active automáticamente el secundario con la misma configuración y estado que el principal. De esta manera se garantiza la continuidad del servicio.

Los firewalls se conectan a la red interna por medio de la VLAN1 configurada en los switches de acceso redundantes Cisco 2960G (SW-PMG-01 y SW-PMG-02). Estos switches también permiten la sincronización de estado entre firewalls a través de la VLAN2.

2.3. Encriptación

La transferencia de datos entre el cliente y el MATba, es codificada usando el algoritmo SHA256 en todo momento. Todas las conexiones cliente/servidor usan encriptación SSL estándar de 2048 bits.

2.4. Autenticación

- La autenticación de los usuarios se realiza mediante Usuario/Password.
- Las Passwords son encriptados en el punto de entrada y son codificadas y almacenadas utilizando el algoritmo SHA-256.
- Las claves son configuradas utilizando el siguiente criterio de seguridad
    - Las claves deben contener 3 de los siguientes 4 tipos (Mayúsculas, minúsculas, números, signos de puntuación).
    - Las claves deben coincidir con un tamaño preestablecido (configurable).
    - Las claves expiran luego de un periodo de tiempo, y deben ser cambiadas por el usuario (configurable).
    - Las claves deben ser distintas a aquellas guardadas en el historial de claves (configurable).

Mercado a Término de Buenos Aires

Por política del MATba, los usuarios son generados utilizando caracteres en mayúscula y minúscula, dado que el sistema distingue entre ambos tipos.