Ciberseguridad en los mercados de valores-Una perspectiva internacional. Mayo 2016.

En la reunión del Consejo de IOSCO, de febrero de 2014, IOSCO acordó apoyar las distintas iniciativas que se estaban analizando en el ámbito de la Ciberseguridad en los mercados de valores reconociendo la necesidad de hacer frente a las amenazas, a la integridad, eficacia y solidez de los mercados financieros en el mundo. La Autoridad de los Mercados Financieros de Quebec (AMF), como coordinadora de los trabajos de varios comités permanentes de IOSCO, y otros participantes en el tema de Ciberseguridad, junto con la ayuda de la Autoridad Monetaria de Singapur (MAS) y la Comisión de Valores de China (CSRC), tomaron parte activa en este tema. Los trabajos realizados orientados, fundamentalmente, a copar con los desafíos en Ciberseguridad a los que se enfrentan los miembros de IOSCO y otros participantes en los mercados de valores, han dado lugar a un informe. Las consideraciones que se incluyen están en una etapa inicial para crear una política unificada en materia de seguridad en términos de identificación de riesgos, protección de medidas técnicas, organizativas y concienciación del personal, detección mediante el control de tráfico de datos (combinando herramientas de software SIEM con servicios de inteligencia prestados por empresas), respuesta, con planes de continuidad de negocio (BCPs) y medidas para asegurar o recuperar la disponibilidad de datos o sistemas, y la recuperación en función de las particularidades de la empresa o sector afectado.

En relación al papel de los supervisores existe una gran diversidad de opciones y prácticas regulatorias que pueden ser útiles y exitosas. El informe aporta ejemplos de regulación en diferentes jurisdicciones (Singapur, Australia, Reino Unido, EEUU) cuyo punto en común es la flexibilidad que suele dejarse a las entidades reguladas a la hora de hacer frente a este problema. También se aportan ejemplos de prácticas seguidas por los participantes en los mercados para identificar, proteger, detectar, responder y recuperarse de ciberataques. Igualmente, el informe trata el tema del intercambio de información apuntando que los Principios y el MMoU de IOSCO dan cobertura a la cooperación entre Autoridades en la investigación de infracciones relacionadas con el cibercrimen.

El informe contiene una introducción al tema de ciberseguridad, siete capítulos y unas conclusiones generales, además de bibliografía y anejos.

En el **capítulo 1**, en el que se hace la introducción, se definen los ciberriesgos, ciberataques, los pasos a tomar por los reguladores y las prácticas de los participantes para mejorar la ciberseguridad. Las nuevas tecnologías tienen ventajas y desventajas, las transacciones de valores se hacen de forma electrónica y por tanto están expuestas a una amenaza constante. Existen organizaciones que no denuncian los ataques para no perder su reputación.
Una encuesta de IOSCO y la Federación Mundial de Bolsas (WFE) descubrió que un 53% de los intercambios de valores fueron afectados y estas amenazas son crecientes. Se han tomado varias iniciativas para enfrentarse a estas amenazas, en Singapur se emitieron directrices, en el Reino Unido se centraron en propuestas para la dirección institucional y en EEUU se puso énfasis en las empresas de inversión registradas.

El **capítulo 2** trata sobre la revelación de incidentes, principios de divulgación periódicos y el tratamiento de

un marco de divulgación en las jurisdicciones de los miembros de IOSCO dependientes de las leyes domésticas. Se recomienda aplicar los estándares existentes en IOSCO diseñados para evitar ciberriesgos.

El **capítulo 3** se centra en los centros de negociación y la recomendación de implementaciones en las negociaciones electrónicas, revisiones periódicas, prácticas seguras y el examen de los marcos actuales aplicados a la ciberseguridad. Se muestran ejemplos de hackers, criminales y posibles ataques terroristas y una lista detallada de la vulnerabilidad de la ciberseguridad, así como el marco NIST (National Institute of Standards and Technology). Las tendencias que surgen de las prácticas de seguridad en los centros de negociación son: a) sistemas de atraer y atrapar; b) información de amenazas en tiempo real; c) herramientas SIEM; d) protección de información interna; e) dirección de terceras partes; f) nuevos enfoques de seguridad en la nube; y g) colaboración con la comunidad de centros de negociación. Se describen igualmente marcos reguladores de la ciberseguridad aplicables a los centros de negociación. Un esbozo de conclusión sobre este tema es que los reguladores usan diferentes roles para asegurar la ciberseguridad y han realizado simulaciones de brechas informáticas como en los miembros de SROs —organizaciones autorreguladas— y clientes institucionales.

El **capítulo 4** trata los intermediarios del mercado. El comité de IOSCO ha formado un grupo de trabajo para proveer asistencia informal sobre este tema que incluye una lista de necesidades básicas, literatura esencial e informes relevantes según las 5 funciones anteriormente señaladas. Se ponen los ejemplos de México y EEUU. Las medidas tomadas por FINRA son dirección de manejo de riesgos en ciberseguridad, evaluación de riesgos, planeamiento de respuestas y la formación de los empleados en ciberinteligencia e informaciones compartidas. No parece haber una medida única en ciberseguridad para todos los miembros.

El **capítulo 5** examina los gestores de activos, en base a la realización de una encuesta con 85 preguntas a los miembros, orientada a proveer a los participantes de datos fidedignos para su uso a nivel de dirección. Entre otros hallazgos destacan: a) asegurarse de que los programas de seguridad de información son consistentes; b) uso de claves largas y complejas; c) inventario periódico de los ordenadores, programas de software y aplicaciones; y d) un plan de respuesta preciso. Los reguladores han tomado medidas distintas a las consideraciones sobre ciberseguridad, unos han enfatizado la dirección, otros los Principios. Los reguladores han comenzado a examinar fallos y las asociaciones industriales han lanzado iniciativas con la organización de seminarios, concienciación, compartiendo experiencias y realizando simulaciones de ataques.

El **capítulo 6** discute las infraestructuras del mercado financiero, el grupo conjunto de CPMI-IOSCO sobre Ciber Resiliencia (WGCR) ha emitido un documento con una guía para las infraestructuras financieras de mercado (FMI) según las categorías de gobernanza, identificación, protección, detección, respuesta y recuperación. Una vez aplicados estos criterios habría que realizar tests, tomar conciencia de la situación y seguir su evolución. El documento propone tomar un papel activo para servir a las partes interesadas y presenta una variada serie de herramientas para mejorar la capacidad cibernética.

El **capítulo 7** expone la necesidad de compartir la información y el rol de los reguladores de valores. La colaboración resulta útil para emular las medidas técnicas de los actores y la prevención de ataques cibernéticos. Existen dos tipos básicos de información, técnica / operacional, es decir, de computadora a computadora, o información estratégica con evidencias contextuales de amenazas o vulnerabilidades. En términos generales, los gobiernos tienen el rol de promover, facilitar y compartir información con la industria estableciendo redes de información. Los participantes en la reunión, sobre esta materia, celebrada en Montreal concluyeron que la información más exitosa provenía del sector privado aunque no es siempre apropiada a toda clase de actores. Debe compartirse la información entre reguladores, paso que IOSCO ha sugerido especialmente en las distintas jurisdicciones. De hecho, y según el MMoU de IOSCO, los reguladores pueden intercambiar información sobre violaciones de seguridad relacionadas con ciberataques. Los miembros del C4 proponen este intercambio de información en casos como ventas fraudulentas, apropiación indebida de bienes, abuso del mercado, disrupción del sistema o sabotaje. El MMoU propone la asistencia mutua dentro de los

Principios relativos a la colaboración que a nivel internacional incluye métodos usados por los criminales, vulnerabilidades, formas de prevención de ataques y tendencias de ciberriesgos.

El **capítulo 8** incluye las siguientes conclusiones generales del informe: a) la ciberseguridad es uno de los retos más importantes para los mercados y reguladores; b) se ofrece una visión de conjunto de los desafíos asociados con la seguridad en los mercados de valores desde una perspectiva internacional; c) existen multitud de amenazas destacando las asociadas al uso de tecnologías de almacenamiento de información y computación en línea; d) se anima a los agentes de los mercados a adoptar medidas y planes expuestos con herramientas, directrices y marcos de actuación; e) la publicación de hechos relevantes sobre ciberriesgos y ciberataques debería ajustarse a las circunstancias particulares de cada emisor, dando suficiente detalle pero sin llegar a comprometer más la ciberseguridad; f) es vital integrar la ciberseguridad en la gobernanza de las entidades implicando a directivos y consejeros; g) la ciberseguridad debe formar parte de los programas de gestión de riesgos; h) es importante compartir información tanto a nivel interno (participantes-reguladores de cada mercado) como, especialmente, internacional, dada la naturaleza internacional de los ciberriesgos; e i) organizaciones como IOSCO pueden estar bien situadas para establecer o promover mecanismos que consigan mayores cotas de intercambio de información.

Finalmente, concluir que el Consejo de IOSCO es consciente de la importancia de la seguridad en el uso de las tecnologías que atañen a los mercados de valores y a sus intervinientes, y por tanto, acordó hacer un seguimiento de esta materia con la propuesta de creación de un grupo de trabajo con el fin de elaborar recomendaciones o buenas prácticas en este entorno.

Para más información, ver el siguiente enlace de interés:
Ciberseguridad en los mercados de valores-Una perspectiva internacional