**Spread the love**

**Un informe del Consejo de  IOSCO de 2016 (basado en otro previo de 2014) alerta sobre aspectos principales de la ciberseguridad en mercados de valores**

1. Define ciberriesgos, ciberataques, decisiones que deben adoptar los reguladores y prácticas de los participantes en mercado para mejorar la ciberseguridad.

2. En relación con 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 y estándares IOSCO para evitar ciberataques

3. En los centros de negociación se deben realizar negociaciones electrónicas, revisiones periódicas, prácticas seguras siguiendo el marco NIST (National Institute of Standards and Technology).
    - sistemas de atraer y atrapar;
    - información de amenazas en tiempo real;
    - herramientas software SIEM;
    - protección de información interna;
    - dirección de terceras partes;
    - nuevos enfoques de seguridad en la nube;
    - colaboración con y entre los centros de negociación.

4. IOSCO cuenta con un grupo de trabajo para proveer asistencia informal a intermediarios de mercado
5. IOSCO realiza encuestas entre gestores de activos para conocer sus necesidades, y ya se conocen algunas
    - Coherencia entre los sistemas de seguridad
    - Claves largas y complejas;
    - Inventario periódico de los ordenadores, programas de software y aplicaciones; y d) un plan de respuesta preciso.

6. Sobre 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): gobernanza, identificación, protección, detección, respuesta y recuperación. Recomienda adoptar un papel activo para mejorar la capacidad cibernética.

7. Se hace preciso compartir información entre 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.
    - Los gobiernos han de promover, facilitar y compartir información con la industria estableciendo redes de información. Según el MMoU de IOSCO, los reguladores pueden intercambiar información sobre violaciones de seguridad relacionadas con ciberataques, particularmente en casos como ventas fraudulentas, apropiación indebida de bienes, abuso del mercado, disrupción del sistema o sabotaje.

8. En conclusión:
    - la ciberseguridad es uno de los retos más importantes para los mercados y reguladores;
    - es un problema internacional, global
    - existen multitud de amenazas destacando las asociadas al uso de tecnologías de almacenamiento de información y computación en línea;
    - los agentes de los mercados deben adoptar medidas basándose en herramientas, directrices y marcos de actuación de IOSCO
    - 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;
    - es vital integrar la ciberseguridad en la gobernanza de las entidades implicando a directivos y consejeros;
    - la ciberseguridad debe formar parte de los programas de gestión de riesgos;
    - es importante compartir información tanto a nivel interno (participantes-reguladores de cada mercado) como, especialmente, internacional, dada la naturaleza internacional de los ciberriesgos;

**IOSCO cuenta con un grupo de trabajo -«*Cyber Resilience and financial technology*» que elabora recomendaciones o buenas prácticas en este entorno.**