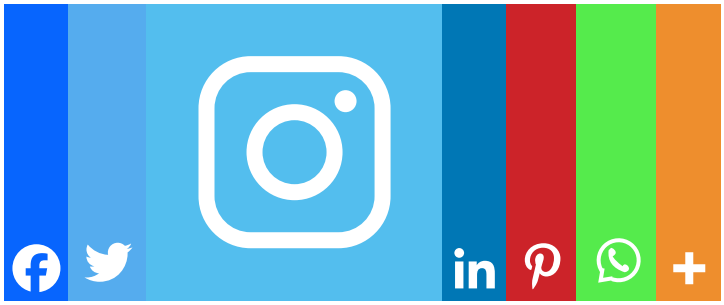
Spread the love



Con motivo de una intervención , estos días, en el I Encuentro INCIBE de Académicos en materia de Ciberseguridad y Derecho, se retoma y actualiza una antigua entrada de agosto de 2017

Decíamos que en EEUU la *Regulation Systems Compliance and Integrity* , RSCI un reglamento que había sido aprobado por la *Securities and Exchange Commission*, SEC, en 2014. El objetivo principal del RSCI es lograr un funcionamiento seguro de los sistemas tecnológicos de los «participantes clave del mercado». La RSCI fue objeto de atención mediática y constituyó una respuesta a los incidentes y fallos en la seguridad y funcionamiento de sistemas informáticos que habían sido comunicados, o que se habían hecho evidentes. De modo muy particular responde a los que condujeron al llamado **flash «crash» de 6 de mayo de 2010.**

La SEC ya -antes de 2015- contaba con una línea de política estratégica de seguridad basada en principios voluntarios (Política de Revisión de la Automatización, ARP) , que incluía inspecciones de vigilancia tecnológica. Además, la *Government Accountability Office* había recomendado introducir normas obligatorias, así como mayores controles y

supervisión de los sistemas informáticos con incidencia en la actividad de los mercados. La RSCI avanza en esa línea:

- Los sistemas de cumplimiento y de integridad a los que refiere a RSCI consisten en **mecanismos informáticos y procedimientos pautados** que se utilizan en procesos digitales desarrollados en los centros de negociación y en su entorno. Se despliegan sobre la negociación, la liquidación, el enrutamiento de ordenes, los datos operativos y de supervisión de mercado, entre otros.
- La RSCI impone que las entidades **aprueben políticas y pongan en marcha procedimientos escritos para proteger su capacidad operativa** (incluyendo pruebas regulares para identificar fallos y amenazas). Deben garantizar que cuentan *con «niveles de capacidad, integridad, resiliencia, disponibilidad y seguridad adecuados para mantener su capacidad operativa, y para interactuar en mercados ordenados*". Se les impone, además, estrictas obligaciones de notificación al supervisor de mercados (SEC), y *de difusión de información entre sus propios administradores y altos ejecutivos, y entre los miembros o partes que se relacionen con la entidad, además de deberes de registro de los incidentes y de las medidas de cumplimento*.
- El vigente Reglamento exige a las entidades sujetas, entre otras cosas: **disponer de políticas y procedimientos** exhaustivos diseñados razonablemente para garantizar que sus sistemas tengan los niveles de **capacidad, integridad, resistencia, disponibilidad y seguridad adecuados** para mantener la **capacidad operativa y promover el mantenimiento de unos mercados justos y ordenados**; adoptar las **medidas correctivas apropiadas** en respuesta a los problemas de los sistemas; **proporcionar notificaciones e informes a la Comisión** diseñados para facilitar la supervisión de la tecnología del mercado de valores; **difundir información sobre los problemas** de los sistemas a las partes afectadas; realizar una **revisión anual** de las políticas y procedimientos de las entidades sujetas. Estas entidades también tendrán que realizar pruebas coordinadas de continuidad de la actividad y pruebas de recuperación en caso de catástrofe (BC/DR), sobre ambas tendrán que crear,

mantener y conservar registros.

- En relación con los marcos tecnológicos, como no existían referencias tecnológicas totalmente fiables se presume que son seguras las disposiciones que se vayan aprobando para el sector financiero por el gobierno de los Estados Unidos u otra «organización ampliamente reconocida"

Actualmente el RSCI entrado en un proceso de reforma: En 2023 la SEC propuso modificaciones al RSCI de la Securities Exchange Act de 1934 («Exchange Act»), cuyo resumen puede consultarse aquí

Paraninfo Gordón Ordás. Universidad de León

Las modificaciones propuestas ampliarían la definición de «entidad sujeta» para incluir una gama más amplia de participantes en las infraestructura del mercado de valores de Estados Unidos, y actualizarían ciertas disposiciones del RSCI para tener en cuenta la evolución del panorama tecnológico de los mercados:

- La ampliación propuesta añadiría las siguientes entidades: los depositarios de datos de permutas financieras basadas en valores («SBSDR», por sus siglas en inglés) registrados; los intermediarios registrados que superen un umbral de activos o de actividad de operaciones; y las agencias de compensación adicionales exentas de registro. Los agentes de bolsa registrados ante la Comisión en virtud de la Sección 15(b) que superen un umbral de activos totales

o un umbral de actividad de transacción en acciones NMS, opciones cotizadas en bolsa, valores del Tesoro de EE.UU. o valores de la Agencia; y – Todas las agencias de compensación exentas de registro.

- Además, las actualizaciones propuestas modificarían las disposiciones del Reglamento en relación con : (i) la clasificación de sistemas y la gestión del ciclo de vida; (ii) la gestión de terceros/proveedores; (iii) la ciberseguridad; (iv) la revisión de la SCI; (v) el papel de las normas industriales actuales; y (vi) el mantenimiento de registros y asuntos relacionados. Sin olvidar que la Comisión ha solicitado comentarios al público sobre si otras entidades, como los intermediarios que utilizan sistemas electrónicos o automatizados para la negociación de valores de deuda corporativa o valores municipales, deben estar sujetos al Reglamento.
- Otras obligaciones que se imponen , de aprobarse la propuesta de reforma, obligan a especificar que las políticas y procedimientos requeridos de una entidad sujeta incluyen: o bien un programa de inventario, clasificación y gestión del ciclo de vida de los sistemas

> SCI y los sistemas SCI indirectos; o bien un programa para gestionar y supervisar a terceros proveedores, incluidos los proveedores de servicios en la nube, que proporcionen o soporten sistemas SCI o SCI indirectos. También, como se indicó antes, que cuenten con Planes de resistencia y recuperación (BC/DR) y que éstos prevean la respuesta para supuestos en los que la indisponibilidad de cualquier proveedor externo sin el cual habría un impacto material en los sistemas SCI críticos; o un programa para evitar el acceso no autorizado a los sistemas SCI y a la información en ellos contenida.

Entradas relacionadas:

> Ciberseguridad en mercados de valores (III) Guia IOSCO de resiliencia cibernética de infraestructuras mercados. Y, otras guías y propuestas

> Ciberseguridad, orientaciones para empresas cotizadas. Antecedentes, a la espera de la reforma normativa en Estados Unidos

> Ciberseguridad en mercados de valores (I). Cooperación internacional y flexibilidad

Ciberseguridad en mercados de valores (II). Informe Consejo IOSCO 2016

Investigación financiada por el proyecto nacional PID2021-127527OB-I00, Proyectos de Generación de Conocimiento 2021, Modalidades: Investigación No Orientada e Investigación Orientada