Comunicado sobre Modificaciones al Reglamento SP, Gestión de Riesgos de Ciberseguridad y Modificaciones al Reglamento SCI

****

**[](https://www.sec.gov/about/commissioners/caroline-a-crenshaw)**

Comisionada Caroline A. Crenshaw

15 de marzo de 2023

Gracias, presidente Gensler, y gracias a mis compañeros comisionados. Las tres propuestas que estamos considerando hoy abordan el papel de la tecnología de la información en los mercados de valores. [[1]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn1%22%20%5Co%20%22) La tecnología ya no es solo fundamental para el funcionamiento de los mercados: son los mercados, y su gestión es vital para la protección de los inversores y las operaciones de mercado justas, ordenadas y eficientes.

Si bien las tres propuestas que estamos considerando hoy están relacionadas, cada una tiene un alcance y propósito únicos: las enmiendas al Reglamento SP abordan la privacidad de los datos y la protección de la información del cliente, la propuesta de Gestión de riesgos de seguridad cibernética se centra en proteger a las entidades del mercado de las amenazas cibernéticas y las enmiendas a La regulación SCI se relaciona con la fortaleza y resiliencia de la infraestructura clave del mercado. En algunos casos, estos diferentes objetivos pueden lograrse por medios similares, por ejemplo, al exigir a las entidades que establezcan políticas y procedimientos para abordar los riesgos de seguridad cibernética. Y puede ser que las entidades del mercado puedan apalancar las mismas acciones para cumplir con más de una regla. Cada uno de los comunicados solicita comentarios sobre si la duplicación creará algún desafío de implementación práctica, y animo a los comentaristas a que nos digan si creen que ese es el caso. Sin embargo, cada una de estas propuestas aborda un aspecto diferente y crítico del papel de la tecnología en los mercados.

***Reglamento SP***

La primera de las tres propuestas presentadas hoy es la modificación del Reglamento SP, que aborda el manejo y la protección de la información personal de los clientes.

Los corredores, asesores de inversiones y otras instituciones financieras almacenan cada vez más información personal de los clientes. En muchos contextos, se requiere el suministro de información personal para acceder a nuestros mercados. Esa información puede pasarse a los proveedores de servicios u otras instituciones financieras sin que los clientes lo sepan. Y si bien el cifrado digital y otras prácticas han fortalecido la protección de esa información personal, también han aumentado la sofisticación y el volumen de actividades delictivas que buscan infiltrarse en las instituciones financieras. [[2]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn2%22%20%5Co%20%22)

Y cuando se roban información personal o activos, los resultados pueden ser calamitosos. Puede conducir al robo de identidad, el robo de ahorros, la ruina del crédito y otros efectos que son personalmente desastrosos para los implicados y que pueden ser sistemáticamente significativos para la economía.

Es por eso que es nuestro imperativo imponer requisitos rigurosos a los registrantes de la SEC y garantizar que la información del cliente esté adecuadamente protegida. Desde el año 2000, el Reglamento SP establece ciertos requisitos para la salvaguardia y disposición adecuada de la información personal. [[3]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn3%22%20%5Co%20%22) La propuesta de hoy se sumaría a las protecciones que actualmente brinda la Regulación SP de manera significativa. Como hemos escuchado hoy, impondría requisitos de protección a los agentes de transferencia, que con frecuencia llegan a poseer información confidencial de los clientes. [[4]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn4%22%20%5Co%20%22)La propuesta requeriría que los registrantes adopten un programa de respuesta a incidentes para abordar el acceso no autorizado o el uso de la información del cliente. Y, lo que es más importante, exigiría ciertos requisitos de notificación al cliente, para garantizar que las personas cuya información confidencial es, o es probable que haya sido violada, sepan sobre la violación y puedan estar en una posición para mitigar el daño. [[5]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn5%22%20%5Co%20%22)

Y, lo que es más importante, si bien muchos estados ya cuentan con ciertas protecciones para los clientes con respecto a la notificación, entre otros asuntos, la propuesta de hoy crearía una línea de base federal. Tener un estándar federal mínimo garantizaría que los clientes en todos los estados sean notificados de cualquier violación de su información confidencial que podría resultar en un daño o inconveniente sustancial.

Muchas gracias al personal de las Divisiones de Negociación y Mercados, Gestión de Inversiones, la División de Análisis Económico y de Riesgos y la Oficina del Asesor Jurídico. Esta propuesta representa un verdadero esfuerzo de colaboración entre divisiones, y la calidad de la propuesta refleja la eficacia de esa colaboración. Estoy feliz de apoyar la propuesta y espero los comentarios del público.

***Gestión de Riesgos de Ciberseguridad***

Como señalé en el pasado, [[6]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn6%22%20%5Co%20%22) la amenaza de ataques cibernéticos en el sistema financiero de EE. UU. es uno de esos problemas que me quita el sueño. Los mercados de valores de EE. UU., en particular, son un componente crítico de nuestra infraestructura económica, con más de un billón de dólares en transacciones que fluyen a través de ellos cada día. [[7]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn7%22%20%5Co%20%22) Eso los convierte en un objetivo atractivo para los ciberdelincuentes que buscan dinero, datos confidenciales o un medio para interrumpir la economía global.

El riesgo de ciberseguridad ha crecido con el tiempo. Los ataques cibernéticos han aumentado en frecuencia y sofisticación, mientras que las entidades del mercado financiero han aumentado su dependencia de la tecnología de la información, incluidas las redes interconectadas, la computación en la nube y las aplicaciones móviles. [[8]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn8%22%20%5Co%20%22)

Debido a que vi los Premios de la Academia el fin de semana pasado, pensé un poco sobre los ataques cibernéticos en las películas de Hollywood. Los piratas informáticos suelen ser los buenos en esas películas, individuos rudos que se infiltran en los sistemas informáticos para corregir un error perpetrado por una institución sin rostro. [[9]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn9%22%20%5Co%20%22) Sin embargo, la realidad no podría ser más diferente. Es mucho más probable que los ataques cibernéticos sean perpetrados por organizaciones criminales o actores asociados con gobiernos extranjeros hostiles, con individuos como víctimas. [[10]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn10%22%20%5Co%20%22)Los ataques cibernéticos representan un riesgo real de daño para los inversores, incluidos los inversores minoristas, por el robo de dinero o información personal confidencial, así como por la pérdida de servicios. Las prácticas sólidas de gestión de riesgos de ciberseguridad son fundamentales, tanto para salvaguardar los fondos y los datos de los inversores como para protegerse contra la posible inestabilidad en todo el mercado.

Como escucharon de mis colegas, la Regla de Gestión de Riesgos de Seguridad Cibernética que estamos considerando hoy se aplicaría a las entidades clave del mercado, incluidas las bolsas de valores nacionales, los corredores de bolsa, las entidades de intercambio basadas en valores, los agentes de transferencia y otros. [[11]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn11%22%20%5Co%20%22) Estas entidades son de fundamental importancia para el funcionamiento justo, ordenado y eficiente de los mercados de valores de EE. UU.

La propuesta requeriría que estas entidades diseñen e implementen políticas y procedimientos de seguridad cibernética para estar mejor preparados para futuras amenazas cibernéticas. Y tales políticas y procedimientos estarían sujetos a requisitos de mantenimiento de registros para que las deficiencias puedan identificarse y abordarse. También estarían obligados, en algunos casos, [[12]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn12%22%20%5Co%20%22) a divulgar los riesgos de seguridad cibernética que anticipan, cómo manejarían esas amenazas y la naturaleza y el alcance de los incidentes de seguridad cibernética significativos que ocurrieron en los últimos dos años. [[13]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn13%22%20%5Co%20%22)

Además, la propuesta requeriría el informe inmediato de cualquier incidente de seguridad cibernética significativo a la Comisión y la divulgación pública inmediata. Esto le daría a la Comisión datos para evaluar tendencias, identificar riesgos emergentes y ayudar a coordinar respuestas a incidentes cibernéticos que tienen el potencial de causar interrupciones más amplias, además de proporcionar al público la información que puede necesitar para responder al incidente. En conjunto, estos requisitos tienen como objetivo mejorar la gestión de riesgos de ciberseguridad para la protección de los inversores y los mercados.

Gracias al personal por todo su arduo trabajo en esta propuesta, en particular al personal de la División de Comercio y Mercados, la División de Análisis Económico y de Riesgos y la Oficina del Asesor Jurídico. Me complace apoyarlo, y espero revisar los comentarios.

***Reglamento SCI***

La historia de los mercados de valores de EE. UU. en las últimas décadas ha sido de automatización, ya que las prácticas comerciales han pasado de ser principalmente manuales a casi completamente electrónicas. [[14]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn14%22%20%5Co%20%22) En reconocimiento de esta transformación fundamental y de la importancia de los sistemas electrónicos para el funcionamiento justo y ordenado de los mercados, en 2014 la Comisión adoptó el Reglamento de Cumplimiento e Integridad de los Sistemas (“Reg SCI”). [[15]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn15%22%20%5Co%20%22) Reg SCI estableció el primer marco integral para la supervisión de la SEC de los sistemas tecnológicos que componen los mercados actuales, con el objetivo de fortalecerlos y mejorar su resiliencia. [[dieciséis]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn16%22%20%5Co%20%22)

Por muchas medidas, está funcionando. Si bien siempre es un desafío demostrar que es negativo al identificar fallas o interrupciones que no ocurrieron, los mercados han demostrado resistencia en los últimos años, incluso durante los volúmenes de negociación sin precedentes y la volatilidad del mercado de principios de 2020. [17] Muchos observadores acreditaron esto [al](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn17%22%20%5Co%20%22) menos en parte a Reg SCI. [[18]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn18%22%20%5Co%20%22) Y aunque algunos errores y fallas son inevitables, no hemos visto repeticiones de eventos como Flash Crash de 2010, la falla de IPO de Facebook de 2012 o los cierres de intercambio de varios días después de la super tormenta Sandy. Es razonable concluir que Reg SCI ha sido un héroe mayormente anónimo de interrupciones del mercado que no ocurrieron.

Sin embargo, los mercados han seguido evolucionando y aumentando su complejidad e interconexión, y la exclusión de ciertas entidades clave del mercado de Reg SCI se ha vuelto cada vez más insostenible. Volúmenes cada vez mayores de transacciones de valores ahora se negocian a la velocidad de la luz en una amplia gama de clases de activos en las plataformas de negociación de la competencia, incluidas las que ofrecen los corredores de bolsa. [[19]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn19%22%20%5Co%20%22) En 2020, la SEC propuso extender Reg SCI a ciertos sistemas de negociación alternativos, o ATS, que negocian valores gubernamentales. [[20]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn20%22%20%5Co%20%22) En 2021, como parte de la adopción de la regla de Infraestructura de datos de mercado, la Comisión modificó el Reglamento SCI para extenderlo a ciertos "consolidadores de la competencia ". [[21]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn21%22%20%5Co%20%22)Hoy, proponemos aprovechar esas acciones anteriores al extender Reg SCI para que se aplique a participantes clave adicionales del mercado, así como actualizar algunas de sus disposiciones.

Específicamente, las enmiendas que estamos considerando hoy extenderían los requisitos de Reg SCI a los repositorios de datos de intercambio basados ​​en valores, ciertos corredores de bolsa registrados y agencias de compensación adicionales. Las enmiendas también fortalecerían ciertos requisitos con respecto a las políticas y procedimientos de las entidades SCI, la supervisión de los proveedores de servicios externos, las revisiones anuales y las pruebas de penetración. Estas mejoras al marco deberían ayudar a garantizar que los sistemas tecnológicos en los que confían las entidades clave del mercado sigan siendo sólidos, resistentes y seguros. [[22]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn22%22%20%5Co%20%22)

Como se propuso originalmente en 2013, Reg SCI habría incluido ATS que negociaban deuda corporativa o valores municipales, si excedían ciertos umbrales de volumen. [[23]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn23%22%20%5Co%20%22) Estas entidades no se incluyeron en la adopción, sobre la base de que estos ATS de renta fija dependían menos de la automatización y el comercio electrónico que los mercados de valores. [[24]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn24%22%20%5Co%20%22) La propuesta de hoy solicitaría comentarios sobre la posible extensión de Reg SCI a esas entidades. Si bien la negociación manual sigue siendo más **frecuente** en los mercados de renta fija en comparación con los mercados de acciones casi totalmente electrónicos, la tecnología para negociar deuda corporativa y valores municipales ha evolucionado a un ritmo rápido. [[25]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn25%22%20%5Co%20%22)Hay muchos datos que indican que las distinciones establecidas por la Comisión en el comunicado de adopción original pueden no ser válidas hoy. [[26]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftn26%22%20%5Co%20%22) Espero escuchar comentarios sobre esta pregunta.

Gracias nuevamente al personal de la División de Comercio y Mercados, la División de Análisis Económico y de Riesgos y la Oficina del Abogado General por su arduo trabajo en este comunicado, y gracias a todo el personal del edificio que trabajó en este paquete de reglas y enmiendas a las reglas. Me complace apoyar estas propuestas y espero revisar los comentarios.

[[1]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref1%22%20%5Co%20%22)Consulte la Regulación S‑P: Privacidad de la información financiera del consumidor y protección de la información del cliente, Comunicado n.º 34-97141; IA-6262; IC-34854 (15 de marzo de 2023) (“Propuesta de Reglamento SP”); Regla de Gestión de Riesgos de Ciberseguridad para Casas de Bolsa, Cámaras de Compensación, Principales Participantes de Swaps Basados ​​en Valores, Junta Municipal de Reglamentación de Valores, Asociaciones Nacionales de Valores, Bolsas Nacionales de Valores, Repositorios de Datos de Swaps Basados ​​en Valores, Agentes de Swaps Basados ​​en Valores y Agentes de Transferencia, Comunicado No. 33-11167 (15 de marzo de 2023) ("Propuesta de Ciberseguridad"); Cumplimiento e integridad de los sistemas de regulación, comunicado n.º 34-97143 (15 de marzo de 2023) ("Propuesta de SCI de regulación").

[[2]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref2%22%20%5Co%20%22)Véase , por ejemplo , Oficina Federal de Investigaciones, [Informe sobre delitos en Internet de 2021](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf) (22 de marzo de 2022, en 7-8) (en el que se indica que el Centro de quejas sobre delitos en Internet del FBI recibió 847 376 denuncias en 2021 (un aumento de aproximadamente el 181 % desde 2017). ))); ver también Orden de la Comisión, [In the Matter of Morgan Stanley Smith Barney LLC](https://www.sec.gov/litigation/admin/2016/34-78021.pdf)*,* Comunicado No. 34-78021 (8 de junio de 2016), (orden resuelta); Orden de la Comisión [, In the Matter of Cambridge Investment Research, Inc., et al](https://www.sec.gov/litigation/admin/2021/34-92806.pdf) ., Comunicado No. 34-92806 (30 de agosto de 2021) (orden resuelta); Orden de la Comisión, [en el asunto de Cetera Advisor Networks LLC, et al](https://www.sec.gov/litigation/admin/2021/34-92800.pdf)., comunicado n.º 34-92800 (30 de agosto de 2021) (orden resuelta); Orden de la Comisión, [In the Matter of KMS Financial Services, Inc.](https://www.sec.gov/litigation/admin/2021/34-92807.pdf) , Comunicado No. 34-92807 (30 de agosto de 2021) (orden resuelta).

[[3]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref3%22%20%5Co%20%22) Consulte Privacidad de la información financiera del consumidor (Reglamento SP), Exch. Ley Rel. No. 42974 (22 de junio de 2000); 17 CFR § 248 y siguientes.

[[4]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref4%22%20%5Co%20%22) La regla propuesta se aplicaría a los agentes de transferencia registrados con la Comisión u otra agencia reguladora apropiada según se define en la Sección 3(a)(34)(B) de la Ley de Bolsa.

[[5]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref5%22%20%5Co%20%22) Los clientes que saben que sus datos han sido violados pueden tomar medidas para proteger sus activos o información personal, como cambiar las contraseñas de las cuentas, implementar alertas de fraude, monitorear su crédito, notificar a otros con acceso conjunto a las cuentas, notificar a otras instituciones financieras dónde pueden tener cuentas (para evitar que se abran nuevas cuentas a su nombre), entre otras medidas para protegerse contra el mal uso de su información y la disipación de sus activos.

[[6]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref6%22%20%5Co%20%22)Véase la Comisionada Caroline Crenshaw, [Declaración en apoyo de un enfoque multifacético de la seguridad cibernética](https://www.sec.gov/news/statement/crenshaw-statement-cybersecurity-030922) (9 de marzo de 2022).

[[7]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref7%22%20%5Co%20%22)Ver Propuesta de Ciberseguridad en 11.

[[8]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref8%22%20%5Co%20%22)Identificación. a las 14

[[9]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref9%22%20%5Co%20%22)Véase, por ejemplo, Robert McMillan, [¿Son los hackers de Hollywood falsos o brillantes?](https://www.computerworld.com/article/2761859/are-hollywood-hackers-bogus-or-bright-.html)(24 de febrero de 2010) (señalando que los hackers son “generalmente presentados como buenos, no malos” en las películas de Hollywood).

[[10]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref10%22%20%5Co%20%22)Véase, por ejemplo, Brian O'Connell, [Ask Experian: Who is Behind Most Data Breaches?](https://www.experian.com/blogs/ask-experian/who-is-behind-most-data-breaches/)(24 de abril de 2018) (observando que, del 73 % de las filtraciones de datos provocadas por “forasteros”, los grupos del crimen organizado perpetuaron el 50 % de los ataques, mientras que el 12 % fueron lanzados por estados nacionales o grupos afiliados).

[[11]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref11%22%20%5Co%20%22) La norma propuesta se aplicaría a los corredores de bolsa, las agencias de compensación, los principales participantes de swaps basados ​​en valores, la Junta Municipal de Reglamentación de Valores, las asociaciones nacionales de valores, las bolsas de valores nacionales, los depósitos de datos de swaps basados ​​en valores, los intermediarios de swaps basados ​​en valores, y Agentes de Transferencia. Ver Propuesta de Ciberseguridad.

[[12]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref12%22%20%5Co%20%22) Ciertos corredores de bolsa más pequeños no están sujetos a las políticas y procedimientos adicionales, informes y requisitos de divulgación. identificación \_ en la Sección II.C.

[[13]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref13%22%20%5Co%20%22) Se requiere que las entidades proporcionen una descripción resumida de cada incidente significativo de seguridad cibernética que haya ocurrido durante el año calendario actual o anterior, si corresponde. identificación en 169.

[[14]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref14%22%20%5Co%20%22)Véase Reglamento SCI Propuesta en 6.

[[15]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref15%22%20%5Co%20%22)Véase [Cumplimiento e integridad de los sistemas de regulación](https://www.sec.gov/rules/final/2014/34-73639.pdf) , comunicado n.º 34-73639 (19 de noviembre de 2014).

[[16]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref16%22%20%5Co%20%22)Identificación.

[[17]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref17%22%20%5Co%20%22)Véase Reglamento SCI Propuesta en 7.

[[18]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref18%22%20%5Co%20%22)Ver, p. ej., FINRA Unscripted, [Market Structure & COVID-19: Manejo de mayor volatilidad y volúmenes](https://www.finra.org/media-center/finra-unscripted/market-structure-covid19-coronavirus) (28 de abril de 2020) (“Creo que la SEC recibe mucho crédito. Hubo una regulación que establecieron un Hace un par de años se llamó Reg SCI, Cumplimiento e integridad de los sistemas de regulación, y requiere que entidades como los intercambios y FINRA, para nuestros sistemas críticos, se aseguren de que tengan la capacidad para resistir los aumentos repentinos de volumen o los aumentos repentinos de volumen, las instalaciones de respaldo, fallan pruebas, todas esas cosas que hay que hacer para tener tecnología de sonido. Creo que estamos viendo los beneficios de eso”.); Shane Remolina, [¿Está el comercio remoto conduciendo a un cambio de paradigma en la mesa de operaciones?](http://www.tradersmagazine.com/departments/buyside/is-remote-trading-leading-to-a-paradigm-shift-on-the-trading-desk/) Traders Magazine (20 de mayo de 2020) (“[L]as empresas financieras estuvieron más preparadas durante el COVID-19 gracias a la Regulación SCI para Sistemas, Cumplimiento e Integridad”).

[[19]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref19%22%20%5Co%20%22)Véase, p. ej., SIFMA, [SIFMA Insights: Electronic Trading Market Structure Primer](https://www.sifma.org/wp-content/uploads/2019/10/SIFMA-Insights-Electronic-Trading-Market-Structure-Primer.pdf) (octubre de 2019) (que resume el historial y las tendencias del comercio electrónico en diferentes mercados). Véase también [SEC Staff Report on Algorithmic Trading in US Capital Markets](https://www.sec.gov/files/marketstructure/research/algo_trading_report_2020.pdf) en 16-19, 37 (5 de agosto de 2020) (en el que se analizan los ATS y los internalizadores de los agentes de bolsa, y otras fuentes internas de liquidez, como las plataformas de un solo agente y libros centrales de riesgos operados por casas de bolsa).

[[20]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref20%22%20%5Co%20%22)Ver [Reglamento ATS para ATS que negocian valores del gobierno de EE. UU., acciones de NMS y otros valores; Reglamento SCI para ATS que negocian valores del Tesoro de EE. UU. y valores de agencias; y Mercados Electrónicos de Bonos Corporativos y Valores Municipales](https://www.sec.gov/rules/proposed/2020/34-90019.pdf) , Comunicado No. 34-90019 (28 de setiembre de 2020). La SEC volvió a proponer las enmiendas en 2022. Ver [Enmiendas con respecto a la definición de "intercambio" y sistemas alternativos de comercio (ATS) que comercian con valores del Tesoro y agencias de EE. UU., acciones del sistema de mercado nacional (NMS) y otros valores, comunicado n.º](https://www.sec.gov/rules/proposed/2022/34-94062.pdf) 34 -94062 (26 de enero de 2022).

[[21]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref21%22%20%5Co%20%22)Consulte [Infraestructura de datos de mercado](https://www.sec.gov/rules/final/2020/34-90610.pdf) , comunicado n.º 34-90610 (9 de diciembre de 2020).

[[22]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref22%22%20%5Co%20%22)Véase Reglamento SCI Propuesta en 9.

[[23]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref23%22%20%5Co%20%22)Véase [Cumplimiento e integridad de los sistemas de regulación](https://www.sec.gov/rules/proposed/2013/34-69606.pdf) , comunicado n.º 34-69007 (8 de marzo de 2013) en 36.

[[24]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref24%22%20%5Co%20%22)Ver [Cumplimiento e integridad de los sistemas de regulación](https://www.sec.gov/rules/final/2014/34-73639.pdf) , comunicado No. 34-73639 (19 de noviembre de 2014) en 70-71.

[[25]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref25%22%20%5Co%20%22)Ver Reglamento SCI Propuesta en 106-107.

[[26]](https://www.sec.gov/news/statement/crenshaw-statement-enhanced-cybersecurity-031523%22%20%5Cl%20%22_ftnref26%22%20%5Co%20%22)Véase , por ejemplo , [SIFMA Insights: US Fixed Income Market Structure Primer](https://www.sifma.org/wp-content/uploads/2018/07/SIFMA-Insights-FIMS-Primer_FINAL.pdf) (julio de 2018) (en el que se analizan varios tipos diferentes de mercados de renta fija, y se señala que la estructura históricamente impulsada por cotizaciones del mercado de corredores de voz se ha movido para adaptarse a los protocolos de libros de órdenes limitadas en los mercados intradistribuidores y protocolos de solicitud de cotización ("RFQ") en los mercados de distribuidor a cliente; y evaluar que "El crecimiento actual [en los mercados de distribuidor a cliente] está permitiendo el crecimiento total en los porcentajes generales de electrificación : UST 70%, Agencia 50%, Repos 50%, IG Corporates 40% y HY Corporates 25%”); ver también Annabel Smith, [Pandemic ve dispararse el comercio electrónico de renta fija en 2021](https://www.thetradenews.com/pandemic-sees-electronic-fixed-income-trading-skyrocket-in-2021/), The Trade (3 de marzo de 2021); Consejo Municipal de Reglamentación de Valores, [*Características de la negociación de valores municipales en sistemas de negociación alternativos y plataformas de corredores de bolsa*](https://msrb.org/sites/default/files/MSRB-Trading-on-Alternative-Trading-Systems.pdf?section=0&video=0&hash=096d6e76ba)(agosto de 2021) (discutiendo el volumen en ATS y plataformas de corredores de bolsa de 2016 a 2021).

