Leyes de Ciberseguridad y Valores



[**Discurso**](https://www.sec.gov/news/speeches-statements?aId=edit-news-type&field_person_target_id=&year=All&speaker=&news_type=Speech)

Leyes de Ciberseguridad y Valores

**[[](https://www.sec.gov/biography/gary-gensler)](https://www.sec.gov/biography/gary-gensler)**

Presidente Gary Gensler

Enero 24, 2022

**Instituto Anual de Regulación de Valores de la Facultad de Derecho Northwestern Pritzker**

Gracias. Es bueno estar con el Instituto Anual de Regulación de Valores. Como es costumbre, me gustaría señalar que mis comentarios son míos, y no estoy hablando en nombre de la Comisión o del personal de la SEC.

Como algunos de ustedes sabrán, a menudo me gusta hablar sobre la fundación de las leyes de valores de nuestra nación en la década de 1930.

Así que, de nuevo, hoy, me gustaría hablar de los años 30, pero esta vez, en realidad me refiero a la *década de 1830*.

En 1834, exactamente un siglo antes de que se estableciera la SEC, los hermanos Blanc en Burdeos, Francia, cometieron el primer hackeo del mundo. Los dos banqueros sobornaron a los operadores de telégrafos para que les informaran sobre la dirección en la que se dirigía el mercado. Por lo tanto, obtuvieron una ventaja de información sobre los inversores que esperaron a que la información llegara en autobús de correo desde París.

Los hermanos no fueron condenados por sus acciones, ya que Francia no tenía una ley contra el mal uso de las redes de datos. [[1]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn1) Los Blanc se embolsaron así sus francos, a quemarropa.

Es posible que se pregunte qué tiene que ver todo esto con la SEC. Bueno, creo que es revelador que el primer ataque de *ciberseguridad* del mundo *involucrara valores.* 

Casi doscientos años después de que los Blanc robaran información sobre los mercados de valores, el sector financiero sigue siendo un objetivo muy real de los ciberataques. Además, se ha integrado cada vez más en la infraestructura crítica de la sociedad.

Como supuestamente dijo una vez el famoso ladrón de bancos Willie Sutton, con respecto a por qué robó bancos: "Porque ahí es donde está el dinero". [[2]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn2)

La interconexión de nuestras redes, el uso de análisis predictivos de datos y el deseo insaciable de datos solo se están acelerando. Los actores estatales y los hackers no estatales por igual a veces intentan apuntar a varias entidades y empresas. ¿Por qué? Para robar datos, propiedad intelectual o dinero; menor confianza en nuestro sistema financiero; perturbar las economías; o simplemente demostrar sus capacidades. Todo esto pone en riesgo nuestras cuentas financieras, ahorros e información privada.

Se estima que el costo económico de los ataques cibernéticos es de al menos miles de millones, y posiblemente en billones, de dólares. [[3]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn3) Los hackers han atacado a corredores de bolsa[[4]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn4), agencias gubernamentales[[5]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn5), procesadores de carne y oleoductos. [[6]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn6) Estos ataques pueden tomar muchas formas, desde denegaciones de servicio hasta malware y ransomware.

No es solo el costo económico, por supuesto. La ciberseguridad es fundamental para la seguridad nacional. Los acontecimientos de las últimas dos semanas en Rusia y Ucrania han puesto de relieve una vez más la importancia de la ciberseguridad para nuestro interés nacional.

**Equipo Cyber**

Recientemente, Jen Easterly, directora de la Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA), dijo que "la ciberseguridad es un deporte de equipo". "Todos y cada uno de nosotros somos miembros del Equipo Cibernético", dijo. [[7]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn7)

La gente del sector privado está en primera línea. Como dijo recientemente el presidente Biden, "la mayor parte de nuestra infraestructura crítica es propiedad y está operada por el sector privado, y el gobierno federal no puede enfrentar este desafío solo". [[8]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn8)

Otras entidades gubernamentales, como la Oficina Federal de Investigaciones y CISA, capitanean Team Cyber, pero la SEC también tiene un papel que desempeñar.

Hoy, participamos en el Consejo de Supervisión de la Estabilidad Financiera (FSOC) y el Comité de Infraestructura de Información Financiera y Bancaria (FBIIC). Trabajamos con nuestros homólogos extranjeros en el Consejo de Estabilidad Financiera (FSB), la Organización Internacional de Comisiones de Valores (IOSCO), el Grupo de Expertos Cibernéticos del G7 y en otros lugares.

Tenemos un papel clave como regulador de los mercados de capitales con respecto a los solicitantes de registro de la SEC, que van desde bolsas y corredores hasta asesores y emisores públicos. Ciber se relaciona con cada parte de nuestra misión de tres partes, y en particular con nuestro objetivo de mantener mercados ordenados.

Tenemos muchas reglas que implican riesgo cibernético, que incluyen, entre otras, la continuidad del negocio, los libros y registros, el cumplimiento, la divulgación, el acceso al mercado y la lucha contra el fraude. [[9]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn9) Nuestra División de Exámenes (EXAMS) ha publicado varias alertas de riesgo y declaraciones sobre temas de ciberseguridad,[[10]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn10) y emitió un informe en 2020 sobre observaciones de ciberseguridad y resiliencia. [[11]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn11) Este trabajo ayuda a los solicitantes de registro de la SEC y al público a prepararse y gestionar algunos de estos riesgos cibernéticos.

Los incidentes cibernéticos, desafortunadamente, ocurren mucho. La historia y cualquier estudio de la naturaleza humana nos dice que van a seguir sucediendo. Dado esto, y la evolución del panorama de riesgos de ciberseguridad, en la SEC estamos trabajando para mejorar la postura general de ciberseguridad y la resiliencia del sector financiero.

**Política**

Aunque gran parte de este trabajo se lleva a cabo en el sector privado y en otras partes del gobierno, al contemplar la política de ciberseguridad en la SEC, lo pienso de tres maneras:

* ciberhigiene y preparación
* notificación de incidentes cibernéticos al gobierno
* en determinadas circunstancias, divulgación al público.

Nuestro trabajo de política de ciberseguridad se relaciona con cuatro grupos de entidades:

* Solicitantes de registro de la SEC en el sector financiero, como corredores de bolsa, compañías de inversión, asesores de inversión registrados y otros intermediarios del mercado
* Empresas públicas
* Proveedores de servicios que trabajan con los solicitantes de registro del sector financiero de la SEC, pero que no están necesariamente registrados en la SEC.
* La propia SEC.

Esperamos colaborar en este trabajo con CISA, FSOC, el sector privado y el resto de Team Cyber.

**Registrantes del Sector Financiero SEC**

Permítanme pasar en primer lugar a nuestros tres proyectos relacionados con los solicitantes de registro del sector financiero.

Cumplimiento e integridad de los sistemas de regulación

En primer lugar, creo que tenemos la oportunidad de refrescar el cumplimiento y la integridad de los sistemas de regulación (Reg SCI). [[12]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn12)

¿Qué es SCI? Es una regla, adoptada en 2014, que cubre un subconjunto de grandes registrantes, incluidas bolsas de valores, cámaras de compensación, sistemas de negociación alternativos, organizaciones autorreguladoras (SRO) y similares: infraestructura financiera que forma parte de la columna vertebral de los mercados de capitales. La Pista de Auditoría Consolidada (CAT), como una instalación de cada una de las SRO participantes, también está sujeta a Reg SCI.

La regla ayuda a garantizar que estas entidades grandes e importantes tengan programas tecnológicos sólidos, planes de continuidad del negocio, protocolos de prueba, copias de seguridad de datos, etc. El objetivo principal de Reg SCI era reducir la ocurrencia de problemas de sistemas y mejorar la resiliencia cuando ocurren.

Mucho ha cambiado, sin embargo, en los ocho años transcurridos desde que la SEC adoptó Reg SCI. Por lo tanto, le he preguntado al personal cómo podríamos ampliar y profundizar esta regla. Por ejemplo, ¿podríamos considerar la aplicación de Reg SCI a otras entidades grandes y significativas que actualmente no cubre, como los mayores creadores de mercado y corredores de bolsa? [[13]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn13)

Con ese fin, en 2020, la Comisión propuso incluir grandes plataformas de negociación del Tesoro bajo el paraguas de SCI. En nuestra próxima reunión de la Comisión, consideraremos si volver a proponer esta norma. [[14]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn14)

Del mismo modo, creo que podría haber oportunidades para profundizar Reg SCI para apuntalar aún más la higiene cibernética de entidades financieras importantes.

**Fondos, asesores y corredores de bolsa**

A continuación, me gustaría discutir el grupo más amplio de registrantes del sector financiero, como compañías de inversión, asesores de inversiones y corredores de bolsa, más allá de los cubiertos por Reg SCI.

Como mencioné anteriormente, este grupo tiene que cumplir con varias reglas que pueden implicar sus prácticas de ciberseguridad, como libros y registros, cumplimiento y regulaciones de continuidad del negocio. Sobre la base de eso, le he pedido al personal que haga recomendaciones para la consideración de la Comisión sobre cómo fortalecer la higiene de ciberseguridad y la notificación de incidentes de los registrantes del sector financiero, teniendo en cuenta la orientación emitida por CISA y otros.

Creo que tales reformas podrían reducir el riesgo de que estos solicitantes de registro no puedan mantener la capacidad operativa crítica durante un incidente significativo de ciberseguridad. [[15]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn15) Creo que podrían ofrecer a los clientes e inversores una mejor información con la que tomar decisiones, crear incentivos para mejorar la ciberhigiene y proporcionar a la Comisión más información sobre los riesgos cibernéticos de los intermediarios.

Privacidad de datos

El siguiente ámbito que involucra a los registrantes del sector financiero es en torno a la privacidad de los datos de los clientes y los clientes y la información personal.

El Congreso abordó este tema en la Ley Gramm-Leach-Bliley de 1999. La Comisión adoptó el Reglamento S-P a raíz de dicha Ley. Requiere corredores de bolsa registrados, compañías de inversión y asesores de inversiones para proteger los registros y la información de los clientes. [[16]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn16) Es la razón por la que, hasta el día de hoy, muchos de nosotros recibimos avisos que nos informan sobre las políticas de privacidad de las empresas.

Más de dos décadas desde que se adoptó reg S-P, una eternidad en el mundo de la ciberseguridad, creo que puede haber oportunidades para modernizar y expandir esta regla. En particular, he pedido al personal recomendaciones sobre cómo los clientes reciben notificaciones sobre eventos cibernéticos cuando se ha accedido a sus datos, como su información de identificación personal. Esto también podría incluir la propuesta de modificar el calendario y el contenido de las notificaciones actualmente requeridas en virtud del Reglamento S-P.

**Empresas Públicas**

A continuación, permítanme pasar a la divulgación de las empresas públicas con respecto al riesgo cibernético y los eventos cibernéticos.

La ganga básica es esta: los inversores pueden decidir qué riesgos desean tomar. Las empresas que recaudan dinero del público tienen la obligación de compartir información con los inversores de forma regular.

Los regímenes de divulgación evolucionan a lo largo de las décadas. La ciberseguridad es un riesgo emergente con el que los emisores públicos deben lidiar cada vez más.

Por lo tanto, he pedido al personal que haga recomendaciones para la consideración de la Comisión en torno a las prácticas de ciberseguridad de las empresas y las divulgaciones de riesgos cibernéticos. Esto puede incluir sus prácticas con respecto a la gobernanza, la estrategia y la gestión de riesgos de ciberseguridad.

Muchos emisores ya proporcionan divulgación de riesgos cibernéticos a los inversores. Creo que tanto las empresas como los inversores se beneficiarían si esta información se presentara de manera coherente, comparable y útil para la toma de decisiones.

Además, le he pedido al personal que haga recomendaciones sobre si y cómo actualizar las divulgaciones de las empresas a los inversores cuando se han producido eventos cibernéticos.

No se equivoquen: las empresas públicas ya tienen ciertas obligaciones cuando se trata de divulgaciones de ciberseguridad. Si se roban los datos de los clientes, si una empresa pagó ransomware, eso puede ser importante para los inversores. Como muestran casos recientes, el hecho de no hacer divulgaciones precisas de incidentes y riesgos de ciberseguridad puede resultar en acciones de cumplimiento. [[17]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn17)

**Proveedores de servicios**

A continuación, permítanme pasar a los proveedores de servicios.

Los proveedores de servicios a menudo desempeñan un papel crítico dentro de nuestro sector financiero. Estos proveedores de servicios van mucho más allá de la nube. Pueden incluir sistemas y proveedores de informes de inversores, proveedores de servicios de oficina intermedia, administradores de fondos, proveedores de índices, custodios, análisis de datos, gestión de operaciones y pedidos, y servicios de precios y otros servicios de datos, entre otros. Muchas de estas entidades pueden no estar registradas en la SEC.

Le he pedido al personal que considere recomendaciones sobre cómo podemos abordar aún más el riesgo de ciberseguridad que proviene de los proveedores de servicios. [[18]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn18) Esto podría incluir una variedad de medidas, como exigir a determinados solicitantes de registro que identifiquen a los proveedores de servicios que podrían plantear tales riesgos. Además, podría incluir responsabilizar a los solicitantes de registro por las medidas de ciberseguridad de los proveedores de servicios con respecto a la protección contra el acceso inadecuado y la información del inversor. Esto podría ayudar a garantizar que no se pierdan importantes protecciones para los inversores y que los servicios clave no se vean interrumpidos, ya que los solicitantes de registro del sector financiero dependen cada vez más de los servicios subcontratados.

Dicho esto, vale la pena señalar que las agencias bancarias regulan y supervisan a los proveedores de servicios externos de ciertos bancos directamente a través de la Ley de Compañías de Servicios Bancarios. Podría valer la pena considerar autoridades similares para los reguladores del mercado.

**La SEC**

Finalmente, para decir lo obvio, la SEC tampoco es inmune a los ciberataques.

El personal de la agencia continúa trabajando para proteger los datos de la SEC y la tecnología de la información, así como los datos de la industria que necesitamos para llevar a cabo nuestra misión. Este trabajo se alinea con la Orden Ejecutiva del presidente Biden sobre la Mejora de la Ciberseguridad de la Nación[[19]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftn19) y las directivas de la Oficina de Administración y Presupuesto.

Además, continuamos evaluando nuestra huella de datos y mejorando nuestros procesos de recopilación de datos para recopilar solo los datos que necesitamos para cumplir con nuestra misión.

**Conclusión**

En conclusión, vivimos en una época de rápidos cambios tecnológicos sujetos a desafíos de ciberseguridad siempre presentes. Estos riesgos cibernéticos tienen implicaciones para el sector financiero, los inversores, los emisores y la economía en general. La SEC tiene un papel que desempeñar, junto con el resto del Equipo Cibernético.

Casi dos siglos después de ese primer hackeo cibernético, creo que podemos pensar en cómo protegernos contra las trampas de ciberseguridad de los años 30, no la década de 1830 o la década de 1930, sino la década de 2030.

[[1]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref1) *Véase*Tom Standage, "The crooked timber of humanity" (5 de octubre de 2017), *disponible en*<https://www.1843magazine.com/technology/rewind/the-crooked-timber-of-humanity>.

[[2]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref2) *Véase*la Oficina Federal de Investigaciones, "Willie Sutton", *disponible en*<https://www.fbi.gov/history/famous-cases/willie-sutton>.

[[3]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref3) *Véase*Jacquelyn Schneider, "A World Without Trust: The Insidious Cyberthreat" (enero/febrero), *disponible en*<https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust>.

[[4]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref4) *Consulte*"Robinhood anuncia incidente de seguridad de datos (actualización)" (16 de noviembre de 2021), *disponible en* <https://blog.robinhood.com/news/2021/11/8/data-security-incident>.

[[5]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref5) *Véase*U.S. Government Accountability Office, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response" (22 de abril de 2021), *disponible en*<https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic>.

[[6]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref6) *Véase*Consejo de Supervisión de la Estabilidad Financiera, "Informe Anual 2021", *disponible en* <https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf>.

[[7]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref7) *Véase*Jen Easterly, "Cybersummit 2021 Keynote Address" (6 de octubre de 2021), *disponible en* <https://www.cisa.gov/cybersummit-2021-session-day-1-welcome-and-opening-remarks> (véase 3:32).

[[8]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref8) *Véase*President Joe Biden, "Comentarios del presidente Biden sobre la mejora colectiva de la ciberseguridad de la nación" (25 de agosto de 2021), *disponible en*<https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/25/remarks-by-president-biden-on-collectively-improving-the-nations-cybersecurity/>.

[[9]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref9) *Véase*U.S. SEC, "Cybersecurity", *disponible en*<https://www.sec.gov/spotlight/cybersecurity>.

[[10]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref10) *Véase*, por ejemplo,"Ciberseguridad: alerta de ransomware", *disponible en*<https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf>.

[[11]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref11) *Véase*"Sec Office of Compliance Inspections and Examinations Publishes Observations on Cybersecurity and Resiliency Practices" (27 de enero de 2020), *disponible en* <https://www.sec.gov/news/press-release/2020-20>.

[[12]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref12) *Véase*U.S. SEC, "Spotlight on Regulation SCI", *disponible en*<https://www.sec.gov/spotlight/regulation-sci.shtml>.

[[13]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref13) De hecho, varios comentaristas en 2014 sugirieron que podríamos considerar agregar requisitos de Reg SCI a otras entidades, incluidos los repositorios de datos de intercambio basados en seguridad, las instalaciones de ejecución de swaps basadas en seguridad y los corredores de bolsa que no son ATS. <https://www.govinfo.gov/content/pkg/FR-2014-12-05/pdf/2014-27767.pdf>, págs. 72363-54.

[[14]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref14) *Véase*"SEC Proposes Rules to Extend Regulations ATS and SCI to Treasuries and Other Government Securities Markets" (28 de septiembre de 2020), *disponible en*<https://www.sec.gov/news/press-release/2020-227>.

[[15]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref15) Los corredores de bolsa que son miembros de la Autoridad Reguladora de la Industria Financiera (FINRA) tienen obligaciones de plan de continuidad del negocio bajo FINRA. *Véase*"4370. Planes de continuidad del negocio e información de contacto de emergencia*", disponible en*<https://www.finra.org/rules-guidance/rulebooks/finra-rules/4370>.

[[16]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref16) *Véase*el "Reglamento S-P", *disponible en*<https://www.sec.gov/spotlight/regulation-s-p.htm>.

[[17]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref17) *Consulte*"SEC Charges Issuer With Cybersecurity Disclosure Controls Failures" (15 de junio de 2021), *disponible en*<https://www.sec.gov/news/press-release/2021-102>, y "SEC Charges Pearson plc for Misleading Investors About Cyber Breach", *disponible en*<https://www.sec.gov/news/press-release/2021-154>.

[[18]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref18) Si bien se centró en los sistemas más críticos, hace ocho años, la SEC abordó las relaciones con terceros al adoptar Reg SCI. Las entidades SCI son "responsables de tener procesos y requisitos establecidos para garantizar que pueda cumplir con los requisitos del Reglamento SCI para sistemas operados en nombre de la entidad SCI por un tercero para ciertas entidades del sector financiero". *Ver*Cumplimiento e Integridad de los Sistemas de Regulación, <https://www.govinfo.gov/content/pkg/FR-2014-12-05/pdf/2014-27767.pdf> p. 72276.

[[19]](https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124" \l "_ftnref19) *Ver*"Orden Ejecutiva sobre la Mejora de la Ciberseguridad de la Nación" (12 de mayo de 2021), *disponible en*<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.