La regla final de la SEC introduce informes digitales de ciberseguridad



Publicado el 8 de septiembre de 2023 por [**Editor**](https://www.xbrl.org/news/sec-final-rule-introduces-digital-cybersecurity-reporting/)

La Comisión de Bolsa y Valores de EE. UU. (SEC) ha publicado su norma final sobre gestión *de riesgos, estrategia, gobernanza y divulgación de incidentes de ciberseguridad* por parte de empresas públicas. Esto requerirá que las empresas realicen divulgaciones anuales sobre gestión, estrategia y gobernanza de riesgos de ciberseguridad, así como divulgaciones adicionales después de cualquier incidente importante de ciberseguridad, utilizando Inline XBRL.

Al introducir datos estructurados y estandarizados, la SEC busca *"hacer que las divulgaciones sean más accesibles para los inversores y otros participantes del mercado y facilitar un análisis más eficiente".* Los comentaristas de la propuesta acogieron con agrado el potencial de extracción y análisis automatizados. Para facilitar la implementación y aliviar cualquier carga adicional de presentación de informes, la SEC ha incorporado fechas de cumplimiento escalonadas para los informes Inline XBRL, cada una de las cuales se aplica un año después del mandato de divulgación inicial.

Esta regla ha resultado controvertida, y algunos cuestionan la idoneidad de una mayor transparencia en un ámbito con posibles sensibilidades comerciales, así como las presiones de tiempo en torno a la divulgación de incidentes. Nuestra opinión, sin embargo, es que aquí, como suele ocurrir, la luz del sol es el mejor desinfectante. Éstas son áreas de riesgo cada vez más importantes donde las partes interesadas requieren información de alta calidad.

*"Ya sea que una empresa pierda una fábrica en un incendio, o millones de archivos en un incidente de ciberseguridad, puede ser importante para los inversores",* dijo el presidente de la SEC, Gary Gensler. *“Actualmente, muchas empresas públicas ofrecen información sobre ciberseguridad a los inversores. Sin embargo, creo que tanto las empresas como los inversores se beneficiarían si esta divulgación se hiciera de una manera más coherente, comparable y útil para tomar decisiones. Al ayudar a garantizar que las empresas divulguen información importante sobre ciberseguridad, las normas actuales beneficiarán a los inversores, las empresas y los mercados que los conectan”.*

[Lea más en el anuncio](https://www.sec.gov/news/press-release/2023-139) de la SEC, [la hoja informativa](https://www.sec.gov/files/33-11216-fact-sheet.pdf) y la [regla](https://www.sec.gov/files/rules/final/2023/33-11216.pdf) final misma.

[CIBERSEGURIDAD](https://www.xbrl.org/tag/cybersecurity/) [INLINE XBRL](https://www.xbrl.org/tag/inline-xbrl/) [SEC](https://www.xbrl.org/tag/sec/) [US](https://www.xbrl.org/tag/us/)

La SEC adopta reglas sobre gestión de riesgos de ciberseguridad, estrategia, gobernanza y divulgación de incidentes por parte de empresas públicas

PARA PUBLICACIÓN INMEDIATA 2023-139

*Washington D.C., 26 de julio de 2023 —*

La Comisión de Bolsa y Valores adoptó hoy reglas que requieren que los solicitantes de registro divulguen los incidentes materiales de ciberseguridad que experimentan y que divulguen anualmente información material sobre su gestión de riesgos de ciberseguridad, estrategia y gobernanza. La Comisión también adoptó normas que exigen a los emisores privados extranjeros que divulguen información comparable.

"Ya sea que una empresa pierda una fábrica en un incendio, o millones de archivos en un incidente de ciberseguridad, puede ser material para los inversores", dijo el presidente de la SEC, Gary Gensler. "Actualmente, muchas empresas públicas proporcionan divulgación de ciberseguridad a los inversores. Sin embargo, creo que tanto las empresas como los inversores se beneficiarían si esta divulgación se hiciera de una manera más consistente, comparable y útil para la toma de decisiones. Al ayudar a garantizar que las empresas divulguen información material de ciberseguridad, las reglas actuales beneficiarán a los inversores, las empresas y los mercados que los conectan".

Las nuevas reglas requerirán que los solicitantes de registro divulguen en el nuevo Punto 1.05 del Formulario 8-K cualquier incidente de ciberseguridad que determinen que es material y que describan los aspectos materiales de la naturaleza, el alcance y el momento del incidente, así como su impacto material o impacto material razonablemente probable en el registrante. Un Formulario 1-K del Artículo 05.8 generalmente vencerá cuatro días hábiles después de que un solicitante de registro determine que un incidente de ciberseguridad es material. La divulgación puede retrasarse si el fiscal general de los Estados Unidos determina que la divulgación inmediata representaría un riesgo sustancial para la seguridad nacional o la seguridad pública y notifica a la Comisión dicha determinación por escrito.

Las nuevas reglas también agregan el Artículo 106 del Reglamento S-K, que requerirá que los solicitantes de registro describan sus procesos, si los hubiera, para evaluar, identificar y gestionar los riesgos materiales de las amenazas de ciberseguridad, así como los efectos materiales o los efectos materiales razonablemente probables de los riesgos de las amenazas de ciberseguridad y los incidentes de ciberseguridad anteriores. El punto 106 también requerirá que los solicitantes de registro describan la supervisión de la junta directiva de los riesgos de las amenazas de ciberseguridad y el papel y la experiencia de la administración en la evaluación y gestión de los riesgos materiales de las amenazas de ciberseguridad. Estas divulgaciones serán requeridas en el informe anual del solicitante de registro en el Formulario 10-K.

Las reglas requieren divulgaciones comparables por parte de emisores privados extranjeros en el Formulario 6-K para incidentes materiales de ciberseguridad y en el Formulario 20-F para la gestión de riesgos de ciberseguridad, estrategia y gobernanza.

Las reglas finales entrarán en vigencia 30 días después de la publicación de la liberación de adopción en el Registro Federal. Las divulgaciones del Formulario 10-K y el Formulario 20-F vencerán a partir de los informes anuales para los años fiscales que finalicen a partir del 15 de diciembre de 2023. Las divulgaciones del Formulario 8-K y el Formulario 6-K vencerán a partir de los últimos 90 días después de la fecha de publicación en el Registro Federal o el 18 de diciembre de 2023. Las compañías de informes más pequeñas tendrán 180 días adicionales antes de que deban comenzar a proporcionar la divulgación del Formulario 8-K. Con respecto al cumplimiento de los requisitos de datos estructurados, todos los solicitantes de registro deben etiquetar las divulgaciones requeridas bajo las reglas finales en Inline XBRL a partir de un año después del cumplimiento inicial del requisito de divulgación relacionado.

*###*



HOJA INFORMATIVA

Divulgaciones de ciberseguridad de empresas públicas; Reglas finales

La Comisión de Bolsa y Valores adoptó reglas finales que requieren la divulgación de incidentes materiales de ciberseguridad en el Formulario 8-K y la divulgación periódica de la gestión, estrategia y gobierno de riesgos de ciberseguridad de un solicitante de registro en informes anuales.

Antecedentes

En marzo de 2022, la Comisión propuso nuevas reglas, enmiendas a las reglas y enmiendas de formularios para mejorar y estandarizar las divulgaciones relacionadas con la gestión del riesgo de ciberseguridad, la estrategia, la gobernanza y los incidentes materiales de ciberseguridad por parte de empresas públicas que están sujetas a los requisitos de información de la Ley de Intercambio de Valores de 1934. La Comisión observó que las amenazas e incidentes de ciberseguridad plantean un riesgo continuo y creciente para las empresas públicas, los inversores y los participantes en el mercado. Señaló que los riesgos de ciberseguridad han aumentado junto con la digitalización de las operaciones de los registrantes, el crecimiento del trabajo remoto, la capacidad de los delincuentes para monetizar los incidentes de ciberseguridad, el uso de pagos digitales y la creciente dependencia de proveedores de servicios externos para los servicios de tecnología de la información, incluida la tecnología de computación en la nube. La Comisión también observó que el coste para las empresas y sus inversores de los incidentes de ciberseguridad está aumentando y lo está haciendo a un ritmo cada vez mayor. Todas estas tendencias subrayan la necesidad de mejorar la divulgación.

La propuesta siguió las orientaciones interpretativas emitidas por el personal de la Comisión en 2011 y por la Comisión en 2018 sobre la aplicación de los requisitos de divulgación existentes a los riesgos e incidentes de ciberseguridad. Aunque las divulgaciones de incidentes materiales de ciberseguridad y la gestión y gobernanza de riesgos de ciberseguridad por parte de los solicitantes de registro han mejorado desde la guía de 2011 y 2018, las prácticas de divulgación son inconsistentes y requieren nuevas reglas. La propuesta tenía por objeto dar lugar a divulgaciones coherentes, comparables y útiles para la toma de decisiones que permitieran a los inversores evaluar la exposición de los solicitantes de registro a riesgos e incidentes materiales de ciberseguridad, así como la capacidad de los solicitantes de registro para gestionar y mitigar esos riesgos.

Qué se requiere

El nuevo Formulario 8-K Ítem 1.05 requerirá que los registrantes divulguen cualquier incidente de ciberseguridad que determinen que es material y describan los aspectos materiales de la naturaleza, el alcance y el momento del incidente, así como el impacto material o el impacto material razonablemente probable del incidente en el registrante, incluida su condición financiera y los resultados de las operaciones.

Los solicitantes de registro deben determinar la materialidad de un incidente sin demora irrazonable después del descubrimiento y, si el incidente se determina material, presentar un Formulario 8-K del Artículo 1.05 generalmente dentro de los cuatro días hábiles posteriores a dicha determinación. La divulgación puede retrasarse si el fiscal general de los Estados Unidos determina que la divulgación inmediata representaría un riesgo sustancial para la seguridad nacional o la seguridad pública y notifica a la Comisión dicha determinación por escrito. Si el fiscal general indica que es necesaria una nueva demora, la Comisión considerará solicitudes adicionales de demora y podrá otorgar dicha reparación a través de posibles órdenes de exención.

El nuevo Reglamento S-K Ítem 106 requerirá que los solicitantes de registro describan sus procesos, si los hubiera, para evaluar, identificar y gestionar los riesgos materiales de las amenazas de ciberseguridad, así como si los riesgos de las amenazas de ciberseguridad, incluso como resultado de incidentes de ciberseguridad anteriores, han afectado materialmente o es razonablemente probable que afecten materialmente al solicitante de registro. El punto 106 también requerirá que los solicitantes de registro describan la supervisión de la junta directiva de los riesgos de las amenazas de ciberseguridad y el papel y la experiencia de la administración en la evaluación y gestión de los riesgos materiales de las amenazas de ciberseguridad.

El Formulario 6-K se modificará para exigir a los emisores privados extranjeros que proporcionen información sobre incidentes materiales de ciberseguridad que hagan o deban hacer públicos o divulguen de otro modo en una jurisdicción extranjera a cualquier bolsa de valores o a los titulares de valores. El Formulario 20-F se modificará para exigir que los emisores privados extranjeros hagan divulgación periódica comparable a la requerida en el nuevo Artículo 106 de la Regulación S-K.

¿Qué sigue?

Las reglas finales entrarán en vigencia 30 días después de la publicación de la liberación de adopción en el Registro Federal. Con respecto al Artículo 106 de la Regulación S-K y los requisitos comparables en el Formulario 20-F, todos los solicitantes de registro deben proporcionar dichas divulgaciones comenzando con informes anuales para los años fiscales que terminan en o después del 15 de diciembre de 2023. Con respecto al cumplimiento de los requisitos de divulgación de incidentes en el Formulario 8-K Punto 1.05 y en el Formulario 6-K, todos los solicitantes de registro que no sean compañías informantes más pequeñas deben comenzar a cumplir más tarde 90 días después de la fecha de publicación en el Registro Federal o el 18 de diciembre de 2023. Las compañías de informes más pequeñas tendrán 180 días adicionales y deben comenzar a cumplir con el Formulario 8-K Ítem 1.05 en el último de los 270 días a partir de la fecha de vigencia de las reglas o el 15 de junio de 2024. Con respecto al cumplimiento de los requisitos de datos estructurados, todos los solicitantes de registro deben etiquetar las divulgaciones requeridas bajo las reglas finales en Inline XBRL a partir de un año después del cumplimiento inicial del requisito de divulgación relacionado.



**Gestión de riesgos de ciberseguridad, estrategia, gobernanza y divulgación de incidentes**

**AGENCIA:** Comisión de Bolsa y Valores.

**ACCIÓN:** Norma definitiva.

**RESUMEN: La Comisión de Bolsa y Valores** ("Comisión") está adoptando nuevas reglas para mejorar y estandarizar las divulgaciones relacionadas con la gestión de riesgos de ciberseguridad, estrategia, gobernanza e incidentes por parte de empresas públicas que están sujetas a los requisitos de presentación de informes de la Ley de Bolsa de Valores de 1934. Específicamente, estamos adoptando enmiendas para exigir la divulgación actual sobre incidentes materiales de ciberseguridad. También estamos adoptando reglas que requieren divulgaciones periódicas sobre los procesos de un solicitante de registro para evaluar, identificar y gestionar los riesgos materiales de ciberseguridad, el papel de la administración en la evaluación y gestión de los riesgos materiales de ciberseguridad, y la supervisión de los riesgos de ciberseguridad por parte de la junta directiva. Por último, las reglas finales requieren que las divulgaciones de ciberseguridad se presenten en Inline eXtensible Business Reporting Language ("Inline XBRL").

**FECHAS:** Fecha de entrada en vigor: Las enmiendas entran en vigencia el 5 de septiembre de 2023. Fechas de cumplimiento: Ver Fechas de cumplimiento.

**PARA OBTENER MÁS INFORMACIÓN, COMUNÍQUESE CON: Nabeel Cheema, Asesor Especial, al (202) 551-3430, en la Oficina de Reglamentación, División de** Finanzas Corporativas; y, con respecto a la aplicación de las reglas a las empresas de desarrollo empresarial, David Joire, Asesor Especial Senior, al (202) 551-6825 o IMOCC@sec.gov, Oficina del Asesor Jurídico, División de Gestión de Inversiones, Comisión de Bolsa y Valores de los Estados Unidos, 100 F Street NE, Washington, DC 20549.

**INFORMACIÓN COMPLEMENTARIA:** Estamos adoptando enmiendas a:



**Introducción y antecedentes**

El 9 de marzo de 2022, la Comisión propuso nuevas reglas, y enmiendas de reglas y formas, para mejorar y estandarizar las divulgaciones relacionadas con la gestión de riesgos de ciberseguridad, la estrategia, la gobernanza y los incidentes de ciberseguridad por parte de empresas públicas que están sujetas a los requisitos de presentación de informes de la Ley de Intercambio.**3** La propuesta siguió la orientación interpretativa sobre la aplicación de los requisitos de divulgación existentes al riesgo e incidentes de ciberseguridad que la Comisión y el personal habían emitido en años anteriores.

En particular, en 2011, la División de Finanzas Corporativas emitió una guía interpretativa que proporciona las opiniones de la División sobre las obligaciones de divulgación de las empresas operativas relacionadas con la ciberseguridad ("Guía del personal de 2011").**4** En esa guía, el personal observó que "aunque ningún requisito de divulgación existente se refiere explícitamente a los riesgos de ciberseguridad y los incidentes cibernéticos, una serie de requisitos de divulgación pueden imponer a los solicitantes de registro la obligación de revelar dichos riesgos e incidentes, y además que la información material sobre los riesgos de ciberseguridad y los incidentes cibernéticos debe divulgarse cuando sea necesario para que otras divulgaciones requeridas, a la luz de las circunstancias en las que se realizan, no sean engañosas.**5** La guía apuntaba específicamente a las obligaciones de divulgación bajo 17 CFR 229.503 (Regulación S-K "Artículo 503 (c)") (Factores de riesgo) (desde entonces se trasladó a 17 CFR 229.105 (Regulación S-K "Elemento 105")), 17 CFR 229.303 (Reglamento S-K "Artículo 303") (Discusión y análisis de la gerencia de la situación financiera y los resultados de las operaciones), 17 CFR 229.101 (Reglamento S-K "Artículo 101") (Descripción del negocio), 17 CFR 229.103 (Reglamento S-K "Artículo 103") (Procedimientos legales) y 17 CFR 229.307 (Controles y procedimientos de divulgación), así como a las Codificaciones de Normas de Contabilidad 350-40 (Software de uso interno), 605-50 (Pagos e incentivos de clientes), 450-20 (Contingencias de pérdidas), 275-10 (Riesgos e incertidumbres) y 855-10 (Eventos posteriores).**6**

En 2018, "a la luz de la creciente importancia de los incidentes de ciberseguridad", la Comisión emitió una guía interpretativa para reforzar y ampliar la Guía del personal de 2011 y también abordar la importancia de las políticas y procedimientos de ciberseguridad, así como la aplicación de prohibiciones de uso de información privilegiada en el contexto de la ciberseguridad ("Comunicado interpretativo de 2018").**7** Además de discutir las disposiciones anteriormente cubiertas en la Guía del Personal de 2011, la nueva guía abordó 17 CFR 229.407 (Regulación S-K "Artículo 407") (Gobierno corporativo), 17 CFR Parte 210 ("Regulación S-X") y 17 CFR Parte 243 ("Regulación FD").**8** El comunicado interpretativo de 2018 señaló que las empresas pueden proporcionar informes actuales en el Formulario 8-K y el Formulario 6-K para mantener la precisión e integridad de las declaraciones efectivas de registro de estanterías, y también aconsejó a las empresas que consideraran si podría ser apropiado aplicar restricciones al uso de información privilegiada durante el período posterior a un incidente y antes de la divulgación.**9**

Como se señaló en la Propuesta de Liberación, las prácticas actuales de divulgación son variadas. Por ejemplo, si bien algunos solicitantes de registro informan incidentes materiales de ciberseguridad, más típicamente en el Formulario 10-K, la revisión de las presentaciones del Formulario 8-K, el Formulario 10-K y el Formulario 20-F por parte del personal de la División de Finanzas Corporativas ha demostrado que las empresas proporcionan diferentes niveles de especificidad con respecto a la causa, el alcance, el impacto y la materialidad de los incidentes de ciberseguridad. Del mismo modo, el personal también ha observado que, si bien la mayoría de los solicitantes de registro que divulgan riesgos de ciberseguridad parecen estar proporcionando dichas divulgaciones en la sección de factores de riesgo de sus informes anuales en el Formulario 10-K, las divulgaciones a veces se incluyen con otras divulgaciones no relacionadas, lo que dificulta que los inversores localicen, interpreten y analicen la información proporcionada.**10**

En la publicación propuesta, la Comisión explicó que una serie de tendencias sustentaban la necesidad de los inversores y otros participantes en los mercados de capitales de disponer de información más oportuna y fiable relacionada con la ciberseguridad de los solicitantes de registro que la producida tras la Guía del personal de 2011 y la Publicación interpretativa de 2018. En primer lugar, una parte cada vez mayor de la actividad económica depende de los sistemas electrónicos, de modo que las interrupciones en esos sistemas pueden tener efectos significativos en los solicitantes de registro y, en el caso de ataques a gran escala, efectos sistémicos en la economía en su conjunto.**11** En segundo lugar, ha habido un aumento sustancial en la prevalencia de incidentes de ciberseguridad, impulsado por varios factores: el aumento del trabajo a distancia impulsado por la pandemia de COVID-19; la creciente dependencia de terceros proveedores de servicios para los servicios de tecnología de la información; y la rápida monetización de los ciberataques facilitados por el ransomware, los mercados negros de datos robados y la tecnología de criptoactivos.**12** En tercer lugar, los costos y las consecuencias adversas de los incidentes de ciberseguridad para las empresas están aumentando; Dichos costos incluyen interrupción del negocio, pérdida de ingresos, pagos de rescate, costos de corrección, responsabilidades con las partes afectadas, costos de protección de ciberseguridad, pérdida de activos, riesgos de litigios y daños a la reputación.**13**

Desde la publicación del Lanzamiento propuesto, estas tendencias han continuado a buen ritmo, con incidentes significativos de ciberseguridad que ocurren en empresas e industrias. Por ejemplo, los actores de amenazas ejecutaron repetida y exitosamente ataques contra empresas de alto perfil en múltiples industrias críticas en el transcurso de 2022 y el primer trimestre de 2023, lo que provocó que la Junta de Revisión de Seguridad Cibernética del Departamento de Seguridad Nacional iniciara múltiples revisiones.**14** Del mismo modo, los actores estatales han perpetrado múltiples ataques de alto perfil, y la reciente inestabilidad geopolítica ha elevado tales amenazas.**15** Un estudio reciente realizado por dos empresas de ciberseguridad encontró que el 98 por ciento de Las organizaciones utilizan al menos un proveedor externo que ha experimentado una violación en los últimos dos años.**16** Además, los desarrollos recientes en inteligencia artificial pueden exacerbar las amenazas de ciberseguridad, ya que los investigadores han demostrado que los sistemas de inteligencia artificial pueden aprovecharse para crear código utilizado en ataques cibernéticos, incluso por actores no versados en programación.**17** En general, la evidencia sugiere que las empresas pueden estar subnotificando incidentes de ciberseguridad.**18**

Desde el punto de vista legislativo, observamos que se produjeron dos acontecimientos significativos tras la publicación de la Propuesta de Liberación. Primero, el Presidente promulgó la Ley de Informes de Incidentes Cibernéticos para Infraestructura Crítica de 2022 ("CIRCIA")**19** el 15 de marzo de 2022, como parte de la Ley de Asignaciones Consolidadas de 2022.**20** La pieza central de CIRCIA es la obligación de informar impuesta a las empresas en sectores definidos de infraestructura crítica.**21** Una vez que la Agencia de Seguridad de Ciberseguridad e Infraestructura ("CISA") adopte las reglas, estas compañías deberán informar los incidentes cibernéticos cubiertos a CISA dentro de las 72 horas posteriores al descubrimiento e informar los pagos de rescate dentro de las 24 horas.**22** Es importante destacar que los informes realizados a CISA de conformidad con CIRCIA permanecerán confidenciales; si bien la información contenida en el mismo puede compartirse entre agencias federales con fines de ciberseguridad, investigación y aplicación de la ley, la información no puede divulgarse públicamente, excepto en forma anónima.**23** Observamos que CIRCIA también ordenó la creación de un "Consejo de Informes de Incidentes Cibernéticos . . . coordinar, eliminar conflictos y armonizar los requisitos federales de notificación de incidentes" (el "CIRC"), del cual la Comisión es miembro.**24** En segundo lugar, el 21 de diciembre de 2022, el Presidente promulgó la Ley de Preparación para la Ciberseguridad de la Computación Cuántica, que ordena al Gobierno Federal adoptar tecnología que esté protegida contra el descifrado por la computación cuántica, una tecnología en desarrollo que puede aumentar la capacidad de procesamiento informático considerablemente y, por lo tanto, hace que el cifrado informático existente sea vulnerable al descifrado.**25**

Recibimos más de 150 cartas de comentarios en respuesta a la Liberación de propuestas.**26** La mayoría de los comentarios se centraron en el requisito de divulgación de incidentes propuesto, aunque también recibimos comentarios sustanciales sobre los requisitos propuestos de gestión de riesgos, estrategia, gobierno y experiencia de la junta. Además, el Comité Asesor para Inversores de la Comisión adoptó recomendaciones («Recomendación IAC») con respecto a la propuesta, declarando que: apoya el requisito de divulgación de incidentes propuesto; apoya los requisitos propuestos de gestión de riesgos, estrategia y divulgación de información sobre la gobernanza; recomienda a la Comisión que reconsidere el requisito propuesto de divulgación de conocimientos especializados en materia de ciberseguridad del consejo de administración; sugiere exigir a las empresas que divulguen los factores clave que utilizaron para determinar la materialidad de un incidente de ciberseguridad notificado; y sugiere extender los requisitos de divulgación propuestos 17 CFR 229.106 (Reglamento S-K "Artículo 106") a las declaraciones de registro.**27**

Estamos haciendo una serie de cambios importantes con respecto a la Propuesta de Liberación en respuesta a los comentarios recibidos. Con respecto a la divulgación de incidentes, estamos reduciendo el alcance de la divulgación, agregando un retraso limitado para las divulgaciones que representarían un riesgo sustancial para la seguridad nacional o la seguridad pública, requiriendo cierta divulgación actualizada de incidentes en un Formulario 8-K modificado en lugar de los Formularios 10-Q y 10-K para los registrantes nacionales, y en el Formulario 6-K en lugar del Formulario 20-F para emisores privados extranjeros ("FPI"),**28** y omitiendo la agregación propuesta de incidentes inmateriales para los análisis de materialidad. Estamos racionalizando los elementos de divulgación propuestos relacionados con la gestión de riesgos, la estrategia y la gobernanza, y no estamos adoptando el requisito propuesto de divulgar la experiencia en ciberseguridad de la junta. La siguiente tabla resume los requisitos que estamos adoptando, incluidos los cambios de la Liberación propuesta, como se describe con más detalle en la Sección II a continuación:**29**

|  |  |
| --- | --- |
| Item | Descripción resumida del requisito de divulgación**30** |
| Regulation S-K Item 106(b) – Risk management and strategy | Los solicitantes de registro deben describir sus procesos, si los hubiera, para la evaluación, identificación y gestión de los riesgos materiales de las amenazas de ciberseguridad, y describir si algún riesgo de las amenazas de ciberseguridad ha afectado materialmente o es razonablemente probable que afecte materialmente su estrategia comercial, los resultados de las operaciones o la condición financiera. |
| Regulation S-K Item 106(c) – Governance | Los solicitantes de registro deben: - Describir la supervisión de la junta de los riesgos de las amenazas de ciberseguridad. - Describir el papel de la dirección en la evaluación y gestión de los riesgos materiales de las amenazas de ciberseguridad. |
| Form 8-K Item 1.05 – Material Cybersecurity Incidents | Los solicitantes de registro deben revelar cualquier incidente de ciberseguridad que experimenten que se determine que es material y describir los aspectos materiales de su: - Naturaleza, alcance y tiempo; y - Impacto o impacto razonablemente probable. Se debe presentar un Formulario 8-K del Artículo 1.05 dentro de los cuatro días hábiles posteriores a la determinación de que un incidente fue material. Un solicitante de registro puede retrasar la presentación como se describe a continuación, si el fiscal general de los Estados Unidos ("fiscal general") determina que la divulgación inmediata representaría un riesgo sustancial para la seguridad nacional o la seguridad pública. Los solicitantes de registro deben modificar un Formulario 8-K anterior del Punto 1.05 para divulgar cualquier información requerida en el Artículo 1.05 (a) que no se determinó o no estaba disponible en el momento de la presentación inicial del Formulario 8-K. |
| Form 20-F | Los FPI deben: - Describir la supervisión de la junta de los riesgos de las amenazas de ciberseguridad. - Describir el papel de la dirección en la evaluación y gestión de los riesgos materiales de las amenazas de ciberseguridad. |
| Form 6-K | Los FPI deben proporcionar en el Formulario 6-K información sobre incidentes materiales de ciberseguridad que divulguen o publiquen de otro modo en una jurisdicción extranjera, a cualquier bolsa de valores o a los titulares de valores. |

En general, seguimos convencidos de que, como se detalla en el comunicado de propuesta: la divulgación insuficiente en relación con la ciberseguridad persiste a pesar de la orientación previa de la Comisión; los inversores necesitan una divulgación de ciberseguridad más oportuna y coherente para tomar decisiones de inversión informadas; y los recientes desarrollos legislativos y regulatorios en otras partes del Gobierno Federal, incluidos los desarrollos posteriores a la emisión de la Liberación Propuesta, como CIRCIA**31** y la Ley de Preparación para la Ciberseguridad de la Computación Cuántica,**32** si bien sirven para fines relacionados, no afectarán el nivel de divulgación pública de ciberseguridad que necesitan los inversores en empresas públicas.

1. 15 U.S.C. 77a y siguientes.

2. 15 U.S.C. 78a y siguientes.

3. Consulte Gestión de riesgos de ciberseguridad, estrategia, gobernanza y divulgación de incidentes, Release No. 33-11038 (9 de marzo de 2022) [87 FR 16590 (23 de marzo de 2022)] ("Propuesta de liberación").

4. Consulte CF Disclosure Guidance: Topic No. 2—Cybersecurity (13 de octubre de 2011), disponible en <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>.

5. Ídem.

6. Ídem.

7. Véase la Declaración y orientación de la Comisión sobre divulgaciones de ciberseguridad de empresas públicas, Release No. 33- 10459 (21 de febrero de 2018) [83 FR 8166 (26 de febrero de 2018)], en 8167.

8. Ídem.

9. Ídem.

10. Véase la sección IV.A infra (donde se señala que las divulgaciones actuales de ciberseguridad aparecen en diversas secciones de los informes periódicos y actuales de las empresas y, a veces, se incluyen con otras divulgaciones no relacionadas).

11. Propuesta de liberación en 16591-16592. Véase también U.S. FINANCIAL STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT (2021), pág. 168, disponible en <https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf> (en el que se concluye que "un incidente de ciberseguridad desestabilizador podría amenazar potencialmente la estabilidad del sistema financiero de EE.UU.").

12. Propuesta de liberación en 16591-16592.

13. Ídem.

14. Ver Departamento de Seguridad Nacional, Junta de Revisión de Seguridad Cibernética para realizar una segunda revisión en Lapsus$ (2 de diciembre de 2022), disponible en: <https://www.dhs.gov/news/2022/12/02/cyber-safety-review-board-conduct-second-review-lapsus>; ver también Tim Starks, El último ataque masivo de ransomware se ha estado desarrollando durante casi dos meses, WASH. POST (27 de marzo de 2023), disponible en <https://www.washingtonpost.com/politics/2023/03/27/latest-mass-ransomware-attack-has-been-unfolding-nearly-two-months/>

15. Véase, por ejemplo, Comunicado de prensa, Oficina Federal de Investigaciones, FBI confirma a los actores cibernéticos de Lazarus Group responsables del robo de moneda Horizon Bridge de Harmony (23 de enero de 2023), disponible en <https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft>; Alert (AA22-257A), Agencia de Seguridad de Ciberseguridad e Infraestructura, Actores cibernéticos afiliados al Cuerpo de la Guardia Revolucionaria Islámica de Irán que explotan vulnerabilidades para la extorsión de datos y el cifrado de discos para operaciones de rescate (14 de septiembre de 2022), disponible en <https://www.cisa.gov/uscert/ncas/alerts/aa22-257a>; National Security Agency et al., Joint Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (20 de abril de 2022), disponible en <https://media.defense.gov/2022/Apr/20/2002980529/-1/1/joint_csa_russian_statesponsored_and_criminal_cyber_threats_to_critical_infrastructure_20220420.pdf>.

16. Security Scorecard, Cyentia Institute and Security Scorecard Research Report: Close Encounters of the Third (and Fourth) Party Kind (1 de febrero de 2023), disponible en <https://securityscorecard.com/research/cyentia-close-encounters-of-the-third-and-fourth-party-kind/>

17. Check Point Research, OPWNAI: AI that Can Save the Day or Hack it Away (19 de diciembre de 2022), disponible en <https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away>.

18. Bitdefender, Whitepaper: Bitdefender 2023 Cybersecurity Assessment (abril de 2023), disponible en https://businessresources.bitdefender.com/bitdefender-2023-cybersecurity-assessment.

19. Ley de Notificación de Incidentes Cibernéticos para Infraestructura Crítica de 2022, Pub. L. No. 117-103, 136 Stat. 1038 (2022).

20. Ley de Asignaciones Consolidadas de 2022, H.R. 2471, 117th Cong. (2022).

21. Los sectores se definen en la Directiva de Política Presidencial / PPD-21, Seguridad y Resiliencia de Infraestructura Crítica (12 de febrero de 2013), como: Químico; Instalaciones comerciales; Comunicaciones; Fabricación crítica; Represas; Base Industrial de Defensa; Servicios de Emergencia; Energía; Servicios financieros; Alimentación y Agricultura; instalaciones gubernamentales; Salud y Salud Pública; Tecnología de la información; reactores, materiales y desechos nucleares; Sistemas de Transporte; Sistemas de agua y aguas residuales. Debido a que estos sectores abarcan algunas empresas privadas y no abarcan todas las empresas públicas, el alcance de CIRCIA es a la vez más amplio y más estrecho que el conjunto de empresas sujetas a las normas que estamos adoptando.

22. 6 U.S.C. 681b(a)(1).

23. 6 U.S.C. 681e. Véase la sección II.A.3 para una discusión de por qué nuestras reglas finales tienen un propósito diferente y no están en desacuerdo con los objetivos de CIRCIA.

24. 6 U.S.C. 681f.

25. Quantum Computing Cybersecurity Preparedness Act, H.R. 7535, 117th Cong. (2022). Más recientemente, la Casa Blanca lanzó una Estrategia Nacional de Ciberseguridad para combatir los riesgos continuos asociados con los ataques cibernéticos. La Estrategia Nacional de Ciberseguridad busca reequilibrar la responsabilidad de defenderse contra las amenazas cibernéticas hacia las empresas en lugar del público en general, y busca realinear los incentivos para favorecer las inversiones a largo plazo en ciberseguridad. Ver comunicado de prensa, Casa Blanca, HOJA INFORMATIVA: La administración Biden-Harris anuncia la Estrategia Nacional de Ciberseguridad (2 de marzo de 2023), disponible en <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>

26. Los comentarios públicos que recibimos están disponibles en https://www.sec.gov/comments/s7-09-22/s70922.htm. El 9 de marzo de 2022, la Comisión publicó la Propuesta de Liberación en su sitio web. El período de comentarios para la Liberación de Propuesta estuvo abierto durante 60 días a partir de la emisión y publicación el SEC.gov y finalizó el 9 de mayo de 2022. Un comentarista afirmó que el plazo para formular observaciones no era suficiente y pidió a la Comisión que lo prorrogara por 30 días. Véase la carta del American Chemistry Council ("ACC"). En octubre de 2022, la Comisión reabrió el período de comentarios para la Liberación de Propuesta y otras reglamentaciones porque ciertos comentarios sobre la Liberación Propuesta y otras reglamentaciones se vieron potencialmente afectados por un error tecnológico en el formulario de comentarios de Internet de la Comisión. Consulte Reenvío de comentarios y Reapertura de los períodos de comentarios para varias publicaciones de reglamentación debido a un error tecnológico al recibir ciertos comentarios, Comunicado No. 33-11117 (7 de octubre de 2022) [87 FR 63016 (18 de octubre de 2022)] ("Comunicado de reapertura"). El comunicado de reapertura se publicó en el sitio web de la Comisión el 7 de octubre de 2022 y en el Registro Federal el 18 de octubre de 2022, y el período de comentarios finalizó el 1 de noviembre de 2022. Algunos comentaristas afirmaron que el período de comentarios para la reapertura de la reglamentación no era suficiente y pidieron a la Comisión que ampliara el período de comentarios para esas reglamentaciones. Véase, por ejemplo, las cartas de los Fiscales Generales de los estados de Montana y otros (24 de octubre de 2022) y la Cámara de Comercio de los Estados Unidos (1 de noviembre de 2022). Hemos considerado todos los comentarios recibidos desde el 9 de marzo de 2022 y no creemos que sea necesaria una extensión adicional del período de comentarios.

27. Consulte el Comité Asesor de Inversores de la Comisión de Bolsa y Valores de EE. UU., Recomendación del Subcomité del Inversor como Propietario y el Subcomité de Divulgación del Comité Asesor de Inversores de la SEC con respecto a la gestión de riesgos de ciberseguridad, estrategia, gobernanza y divulgación de incidentes (21 de septiembre de 2022), disponible en <https://www.sec.gov/spotlight/investor-advisory-committee-2012/20220921-cybersecurity-disclosurerecommendation.pdf>. El Comité Asesor de Inversores también celebró una mesa redonda sobre ciberseguridad en su reunión del 10 de marzo de 2022. Véase el Comité Asesor de Inversores de la Comisión de Bolsa y Valores de los Estados Unidos, Agenda de la reunión (10 de marzo de 2022), disponible en [https://www.sec.gov/spotlight/investor-advisory-committee/iac031022- agenda.htm](https://www.sec.gov/spotlight/investor-advisory-committee/iac031022-%20agenda.htm).

28. Un FPI es cualquier emisor extranjero que no sea un gobierno extranjero, excepto un emisor que (1) tenga más del 50 por ciento de sus valores con derecho a voto en circulación registrados por residentes de los Estados Unidos; y (2) cualquiera de los siguientes: (i) la mayoría de sus funcionarios ejecutivos o directores son ciudadanos o residentes de los Estados Unidos; (ii) más del 50 por ciento de sus activos están ubicados en los Estados Unidos; o (iii) su negocio se administra principalmente en los Estados Unidos. 17 CFR 230.405. Véase también 17 CFR 240.3b-4(c).

29. La información que figura en este cuadro no es exhaustiva y sólo pretende destacar algunos de los aspectos más significativos de las modificaciones finales. No refleja todas las enmiendas ni todas las normas y formularios que se ven afectados por las enmiendas finales, que se examinan en detalle a continuación. Como tal, esta tabla debe leerse junto con todo el comunicado, incluido el texto reglamentario.

30. Para los propósitos de este comunicado, los términos "compañías públicas", "compañías" y "registrantes" incluyen emisores que son compañías de desarrollo de negocios según se define en la sección 2(a)(48) de la Ley de Compañías de Inversión de 1940, que son un tipo de compañía de inversión cerrada que no está registrada bajo la Ley de Compañías de Inversión, pero no incluyen compañías de inversión registradas bajo esa Ley.

31. Nota 19 supra.

32. Nota 25 supra.