Divulgación de ciberseguridad



Erik Gerding

*Director de la División de Finanzas Corporativas*

14 de diciembre de 2023

Como es habitual, hoy expreso mis puntos de vista en mi calidad oficial de director de la División de Finanzas Corporativas de la SEC, y mis puntos de vista no reflejan necesariamente los puntos de vista de la Comisión, de ninguno de los Comisionados ni de ningún otro miembro del personal de la Comisión.

En julio de este año, la Comisión adoptó normas definitivas que exigirán a las empresas públicas que divulguen tanto los incidentes materiales de ciberseguridad que experimenten como, anualmente, información importante sobre su gestión de riesgos de ciberseguridad, estrategia y gobernanza. [[1]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn1%22%20%5Co%20%22) Estas normas proporcionarán a los inversores información oportuna, coherente y comparable sobre un importante conjunto de riesgos que pueden causar pérdidas significativas a las empresas públicas y a sus inversores. Esta divulgación puede ayudar a los inversores a evaluar esos riesgos a la hora de tomar decisiones de inversión y voto.

Al recomendar estas reglas finales, el personal de la División de Finanzas Corporativas, junto con el personal de toda la Comisión, consideraron cuidadosamente los comentarios que la Comisión recibió[[2]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn2%22%20%5Co%20%22) sobre las reglas propuestas de marzo de 2022. [[3]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn3%22%20%5Co%20%22) La Comisión tuvo en cuenta estos comentarios, incluidas las preocupaciones sobre el cumplimiento y los actores de amenazas, al decidir realizar cambios en la propuesta y al elaborar un conjunto de normas que promuevan nuestros objetivos de proteger a los inversores y facilitar la formación de capital.

Dado que algunos de los nuevos requisitos de divulgación entrarán en vigor a finales de este mes, es importante subrayar los cambios que la Comisión ha introducido con respecto a la propuesta, destacar algunas partes importantes de la justificación y la mecánica de estas normas y aclarar posibles conceptos erróneos.

**1. Descripción general de la norma y su fundamentación**

La Comisión y su personal llevan muchos años abordando la divulgación de información sobre riesgos de ciberseguridad. En 2011, el personal —y en 2018, la propia Comisión— publicaron orientaciones sobre cómo se aplican las normas de divulgación vigentes a los riesgos e incidentes de ciberseguridad. Aunque la divulgación por parte de las empresas públicas de incidentes materiales de ciberseguridad y la gestión y gobernanza de riesgos de ciberseguridad mejoraron desde que se publicó esa guía, las prácticas de divulgación han seguido siendo incoherentes. Por lo tanto, la Comisión determinó que las nuevas normas proporcionarían a los inversores la información más oportuna, coherente, comparable y útil para la toma de decisiones que necesitan para tomar decisiones informadas sobre inversiones y votos.

La Comisión ha observado que los riesgos de ciberseguridad han aumentado junto con la proporción cada vez mayor de la actividad económica que depende de los sistemas electrónicos, el crecimiento del trabajo a distancia, la capacidad de los delincuentes para monetizar los incidentes de ciberseguridad, el uso de pagos digitales y la creciente dependencia de terceros proveedores de servicios para los servicios de tecnología de la información, incluida la tecnología de computación en nube. En mi opinión, la inteligencia artificial y otras tecnologías pueden mejorar tanto la capacidad de las empresas públicas para defenderse de las amenazas de ciberseguridad como la capacidad de los actores de amenazas para lanzar ataques sofisticados. La Comisión también observó que el coste de los incidentes de ciberseguridad para las empresas y sus inversores está aumentando a un ritmo cada vez mayor. Todas estas tendencias ponen de relieve la necesidad de los inversores de mejorar la divulgación.

Las reglas finales responden a esta necesidad. Al mismo tiempo, es importante subrayar lo que estas normas no hacen para hacer frente a un posible concepto erróneo. La Comisión no pretende prescribir defensas, prácticas, tecnologías, gestión de riesgos, gobernanza o estrategia de ciberseguridad en particular. Las empresas que cotizan en bolsa tienen la flexibilidad de decidir cómo abordar los riesgos y amenazas de ciberseguridad en función de sus propios hechos y circunstancias particulares. Sin embargo, los inversores han indicado que necesitan información coherente y comparable para evaluar el éxito con el que lo están haciendo las empresas públicas.

Para ayudar a los inversores a evaluar esto, la norma final tiene dos componentes: el requisito de revelar los incidentes materiales de ciberseguridad cuatro días hábiles después de que una empresa pública determine que el incidente es material y el requisito de divulgar anualmente información sobre la gestión, la estrategia y la gobernanza de los riesgos de ciberseguridad. Discutiré cada uno de estos requisitos a su vez.

**2. La Disposición de Divulgación de Incidentes de Ciberseguridad**

Para comprender el requisito de divulgación de incidentes de ciberseguridad, es útil plantear y responder a tres preguntas: qué debe divulgarse, cuándo debe divulgarse esa información y por qué la Comisión utilizó un estándar de importancia relativa.

*¿Qué se debe divulgar?* La norma final exige a las empresas públicas que divulguen la ocurrencia de un incidente material de ciberseguridad 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 la empresa, incluida su situación financiera y los resultados de las operaciones. Esta divulgación se centra en los impactos materiales de un incidente de ciberseguridad material. Es más limitado que lo que la Comisión propuso originalmente, que habría requerido detalles adicionales que no estuvieran explícitamente limitados por la importancia relativa. Al revisar el requisito de divulgación, la Comisión tuvo en cuenta no solo los costes de cumplimiento de la empresa, sino también su necesidad de responder y remediar los incidentes. La regla final contiene una instrucción que dice:

Un registrante no necesita divulgar información específica o técnica sobre su respuesta planificada al incidente o sus sistemas de ciberseguridad, redes y dispositivos relacionados, o posibles vulnerabilidades del sistema con tal detalle que impida la respuesta del registrante o la remediación del incidente. [[4]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn4%22%20%5Co%20%22)

De este modo, la Comisión equilibró la necesidad de divulgación con el riesgo de que la divulgación de información técnica específica pudiera proporcionar una hoja de ruta que los agentes de amenazas pudieran aprovechar para futuros ataques.

*¿Cuándo debe divulgarse?* Las empresas públicas deben proporcionar la divulgación requerida del incidente de ciberseguridad dentro de los cuatro días hábiles posteriores a que la empresa determine que el incidente es material. El plazo *no* es de cuatro días hábiles después de que ocurrió o se descubrió el incidente. Este tiempo reconoce que, en muchos casos, una empresa no podrá determinar la materialidad el mismo día en que se descubre el incidente. Una empresa pública puede alertar a empresas en situación similar, así como a actores gubernamentales, en cualquier momento de su respuesta a incidentes, incluso inmediatamente después de descubrir un incidente y antes de determinar la importancia relativa, siempre que no retrase injustificadamente sus procesos internos para determinar la importancia relativa. La Comisión había propuesto un estándar "tan pronto como sea razonablemente posible", pero lo cambió para exigir una determinación de importancia relativa para un incidente de ciberseguridad "sin demora irrazonable". El criterio de "sin demoras injustificadas" de la norma definitiva tenía por objeto abordar las preocupaciones de los comentaristas en relación con el momento de la determinación de importancia relativa. Como reconoció la Comisión en el comunicado de adopción, "una determinación de importancia relativa requiere un proceso informado y deliberativo". [[5]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn5%22%20%5Co%20%22)

Algunos se han preguntado por qué la Comisión eligió cuatro días hábiles como plazo para la divulgación. Este momento es consistente con la notificación de otros eventos que la Comisión requiere que se informen en un Formulario 8-K, como la entrada o terminación de un acuerdo material definitivo o una quiebra. Al adoptar el plazo de cuatro días hábiles, la Comisión explicó que la divulgación de incidentes de ciberseguridad no era lo suficientemente diferente de otros eventos de notificación del formulario 8-K como para justificar un enfoque diferente.

La Comisión también reconoció que una empresa puede no tener información completa sobre el incidente, incluso si sabe lo suficiente como para determinar que el incidente fue importante. Si la empresa no conoce toda la información que debe divulgarse cuatro días hábiles después de una determinación de importancia relativa, la norma final contiene un mecanismo para que la empresa divulgue esa información en una presentación posterior. [[6]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn6%22%20%5Co%20%22)

*¿Por qué utilizar un estándar de materialidad?* También he escuchado a algunas personas, tal vez menos familiarizadas con las leyes federales de valores, preguntar por qué el estándar de divulgación aquí se limita a incidentes de ciberseguridad "materiales". Algunos parecen preferir una regla de línea más brillante. La materialidad es una piedra de toque de las leyes de valores. Conecta las divulgaciones con las necesidades de los inversores. No pretendo sugerir que todas las divulgaciones requeridas por las leyes federales de valores tengan o deban tener un calificador de materialidad. Algunas divulgaciones requeridas no lo hacen.[[7]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn7%22%20%5Co%20%22) En este caso, la Comisión determinó que un calificador de importancia relativa era apropiado. En mi opinión, esto tiene sentido si se tiene en cuenta que algunas empresas pueden sufrir ciberataques a diario, si no con más frecuencia.

Tanto en el comunicado de adopción como en el comunicado de propuesta,[8] la Comisión afirmó que el estándar de materialidad que las empresas deben aplicar para la divulgación de incidentes de ciberseguridad es el mismo estándar articulado por la Corte Suprema en casos como *TSC Industries*, Inc. v. Northway, [9] Basic, Inc. v. *Levinson*[,[10]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn10%22%20%5Co%20%22) y *Matrixx Initiatives, Inc. v. Siracusano,*[[11](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn11%22%20%5Co%20%22)[]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn8%22%20%5Co%20%22) así como en las reglas de la Comisión. [[12]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn12%22%20%5Co%20%22) La Comisión se negó a adoptar una nueva norma de importancia relativa exclusiva de la ciberseguridad. El uso de este estándar de materialidad conocido y probado en el tiempo, en lugar de un nuevo estándar a medida, es coherente con la razón general de la norma: proporcionar a los inversores información para ayudar a evaluar los riesgos de sus inversiones, de la misma manera que reciben información coherente y comparable sobre otros riesgos a los que se enfrentan las empresas públicas.

**3. La Disposición de Demora de Seguridad Nacional y Seguridad Pública**

En la regla final, la Comisión también dispuso la demora en la notificación de divulgaciones de incidentes de seguridad cibernética que representarían un riesgo sustancial para la seguridad nacional o la seguridad pública, dependiendo de una notificación por escrito del fiscal general, quien puede tomar en consideración los hallazgos de otras agencias federales u otras agencias de aplicación de la ley. La Comisión adoptó esta disposición en respuesta a los comentarios recibidos sobre la norma propuesta. Observo que el Departamento de Justicia (DOJ, por sus siglas en inglés) emitió recientemente directrices que describen el proceso que debe seguir una empresa para obtener un aplazamiento y los procedimientos que utilizará el fiscal general para evaluar si se justifica un aplazamiento. [[13]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn13%22%20%5Co%20%22) De acuerdo con las directrices del Departamento de Justicia, las oficinas de campo de la Oficina Federal de Investigaciones (FBI) serán los principales puntos de contacto para las empresas que hayan experimentado incidentes de ciberseguridad. [[14]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn14%22%20%5Co%20%22)

A principios de esta semana, la División de Finanzas Corporativas también emitió una Interpretación de Cumplimiento y Divulgación (CDI, por sus siglas en inglés) para aclarar si las empresas que consultan con el Departamento de Justicia, que incluye al FBI, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés) y cualquier otra agencia de aplicación de la ley o de seguridad nacional sobre un incidente de seguridad cibernética, significa automáticamente que ese incidente debe ser material. [[15]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn15%22%20%5Co%20%22) El texto de este C&DI es el siguiente:

Pregunta: ¿El mero hecho de que un solicitante de registro consulte con el Departamento de Justicia sobre la disponibilidad de una demora en virtud del punto 1.05(c) daría lugar necesariamente a la determinación de que el incidente es importante y, por lo tanto, está sujeto a los requisitos del punto 1.05(a)?

Respuesta: No. Como declaró la Comisión en el comunicado de adopción, la determinación de si un incidente es material se basa en todos los hechos y circunstancias pertinentes que rodean el incidente, incluidos los factores cuantitativos y cualitativos, y debe centrarse en la noción tradicional de materialidad articulada por el Tribunal Supremo.

Además, los requisitos del punto 1.05 no impiden que un registrante consulte con el Departamento de Justicia, incluido el FBI, la Agencia de Seguridad de Infraestructura y Ciberseguridad o cualquier otra agencia de aplicación de la ley o de seguridad nacional en cualquier momento con respecto al incidente, incluso antes de que se complete una evaluación de materialidad.

Espero que esto subraye que la norma no desincentive a las empresas públicas a consultar con las fuerzas del orden o las agencias de seguridad nacional sobre incidentes de ciberseguridad. De hecho, animaría a las empresas públicas a trabajar con el FBI, la CISA y otras agencias de aplicación de la ley y de seguridad nacional lo antes posible después de que se produzcan incidentes de ciberseguridad. Creo que este compromiso oportuno redunda en interés de los inversores y del público. Si bien esto no está dentro del ámbito del personal de la Comisión, las empresas y las agencias gubernamentales pueden encontrar que ese compromiso oportuno podría ayudarlos a determinar más adelante si solicitan un aplazamiento al Departamento de Justicia.

Las consultas con los organismos nacionales de seguridad y de aplicación de la ley pueden, por supuesto, ayudar a las empresas a comprender mejor el impacto o la gravedad de un incidente en particular y, por lo tanto, a evaluar si el incidente es importante. Pero, en última instancia, es responsabilidad de la empresa hacer una determinación de materialidad basada en la consideración de todos los hechos y circunstancias relevantes. En este sentido, vale la pena tener en cuenta que los análisis de incidentes de ciberseguridad por parte de estas otras agencias pueden tener en cuenta factores distintos a un enfoque en un inversor razonable. Esto es coherente con el CDI anterior. Y, como señalé anteriormente, la Comisión no estableció un cronograma fijo para hacer una determinación de importancia relativa, y la consulta de una empresa con cualquier seguridad nacional o aplicación de la ley no cambia esto y pone en marcha el reloj en un cronograma fijo con respecto a un incidente de ciberseguridad. Una vez más, en lugar de un cronograma fijo, la Comisión incluyó la Instrucción 1 en el punto 1.05, que establece que "la determinación de importancia relativa de un solicitante de registro con respecto a un incidente de ciberseguridad debe realizarse sin demora injustificada después del descubrimiento del incidente". [[16]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn16%22%20%5Co%20%22)

**4. Las disposiciones sobre divulgación de información sobre gestión de riesgos, estrategia y gobernanza**

La norma también exige que las empresas públicas divulguen anualmente su gestión de riesgos de ciberseguridad, su estrategia y su gobernanza. Reconociendo las preocupaciones de los comentaristas, la Comisión simplificó la divulgación de información requerida, en comparación con la propuesta, para evitar ser excesivamente prescriptiva o empoderar a los actores de amenazas en detrimento de las empresas y sus inversores.

Por ejemplo, en la norma final, la Comisión eliminó un requisito propuesto de que las empresas públicas revelen si algún miembro de su junta directiva tiene experiencia en ciberseguridad. Los comentaristas expresaron su preocupación de que la propuesta pudiera presionar inadvertidamente a las empresas para que retuvieran a un experto en la junta directiva, y que la inversión en dicho experto podría producirse a expensas de otras inversiones en ciberseguridad u otras prioridades para la supervisión de la junta. En su lugar, la norma final se centra en la divulgación de información sobre el papel de la dirección en la evaluación y gestión de los riesgos materiales derivados de las amenazas a la ciberseguridad, incluyendo, según corresponda, si los puestos de gestión o los comités son responsables de las amenazas a la ciberseguridad y cuáles, así como su experiencia pertinente. Por el contrario, el requisito de divulgación de la regla final con respecto a la junta es de más alto nivel, centrado en describir la supervisión de la junta de los riesgos de las amenazas de ciberseguridad y, si corresponde, identificar cualquier comité o subcomité relevante de la junta y describir cómo se informa a la junta o a dicho comité de dichos riesgos.

Del mismo modo, mientras que la propuesta habría exigido la divulgación de las políticas y procedimientos de ciberseguridad de una empresa pública, así como ciertos detalles específicos relativos a dichas políticas y procedimientos, la norma final se centra de forma más amplia en los procesos de ciberseguridad de la empresa, si los hubiera, e incluye una lista no exclusiva de elementos de divulgación. Esta formulación reconoce que las empresas tendrán diversos enfoques de la ciberseguridad, en función de sus circunstancias particulares, y que no todas las empresas necesitan políticas y procedimientos formales.

**5. Próximos pasos**

A medida que las reglas finales comiencen a entrar en vigor, reconocemos que las empresas públicas trabajarán para garantizar su cumplimiento. Esto podría implicar fomentar conversaciones entre los directores de seguridad de la información, otros expertos y tecnólogos en ciberseguridad de una empresa, el comité de divulgación de la empresa y los responsables de asesorarlos sobre el cumplimiento de la ley de valores. A medida que surgen preguntas interpretativas, quisiera hacer hincapié en la política de puertas abiertas de larga data de la División. Venga a hablar con el personal sobre sus preguntas. Reconocemos que la divulgación pertenece a las empresas públicas y que las empresas públicas y sus asesores están en la primera línea de la divulgación e información a los inversores.

El personal de la Comisión también está ocupado trabajando. Estamos trabajando no solo para responder preguntas y explicar la regla, sino también para preparar a los abogados y contadores de nuestro Programa de Revisión de Divulgaciones para revisar las divulgaciones. Para nuestro Programa de Revisión de Divulgación, el primer año de una regla es muy importante. Pero quiero asegurarles a las empresas y a sus representantes que nuestra División no busca hacer comentarios de "trampa" o penalizar las faltas en los pies. En la medida en que sea apropiado, podemos emitir comentarios prospectivos a empresas o CDI adicionales. Este es un mensaje similar al que yo y otros miembros de la División hemos dado con respecto a otras normas de divulgación que han entrado en vigor recientemente, como las normas de remuneración frente a desempeño. [[17]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftn17%22%20%5Co%20%22) Reconozco el valor de crear incentivos para los esfuerzos de buena fe para cumplir con las nuevas reglas, y espero que este mensaje y el historial de nuestra División con respecto a esas otras reglas brinden tranquilidad a las empresas y sus asesores, particularmente en el primer año de vigencia de esta regla.

Al recomendar nuevos requisitos de divulgación a la Comisión, nuestro objetivo como personal no es simplemente tener otra regla en los libros, simplemente agregar a la "lista de verificación" de cumplimiento de una empresa o inducir divulgaciones repetitivas. Más bien, esperamos obtener divulgaciones personalizadas que proporcionen información consistente, comparable y útil para la toma de decisiones a los inversionistas, en este caso sobre riesgos que realmente no existían (o al menos no existían en la forma actual y en la medida actual) cuando comencé a ejercer como abogado hace varias décadas. Incluso cuando un riesgo es emergente o está evolucionando, las normas de divulgación pueden proporcionar los mismos beneficios en términos de protección de los inversores y formación de capital que tienen para los riesgos a los que se han enfrentado las empresas públicas durante décadas.

[[1](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref1%22%20%5Co%20%22)] *Gestión de Riesgos de Ciberseguridad, Estrategia, Gobernanza y Divulgación de Incidentes,* [Comunicado n.º 33-11216; 34-97989](https://www.sec.gov/rules/2022/03/cybersecurity-risk-management-strategy-governance-and-incident-disclosure#33-11216) (26 de julio de 2023) [88 FR 51896 (4 de agosto de 2023)] ("Adopción de la versión").

[[2]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref2%22%20%5Co%20%22) Los comentarios públicos recibidos por la Comisión sobre las normas propuestas pueden consultarse en <https://www.sec.gov/comments/s7-09-22/s70922.htm>.

[[3](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref3%22%20%5Co%20%22)] *Gestión de riesgos de ciberseguridad, estrategia, gobernanza y divulgación de incidentes,* [Comunicado n.º 33-11038 (9](https://www.sec.gov/rules/2022/03/cybersecurity-risk-management-strategy-governance-and-incident-disclosure#33-11038) de marzo de 2022) [87 FR 16590 (23 de marzo de 2022)] ("Propuesta de publicación").

[[4]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref4%22%20%5Co%20%22) Instrucción 4 al punto 1.05 del formulario 8-K.

[[5]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref5%22%20%5Co%20%22) Adoptando el comunicado en 51906.

[[6]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref6%22%20%5Co%20%22) *Véase*la Instrucción 2 del Punto 1.05 del Formulario 8-K ("En la medida en que la información requerida en el Punto 1.05(a) no esté determinada o no esté disponible en el momento de la presentación requerida, el registrante deberá incluir una declaración a tal efecto en la presentación y luego deberá presentar una enmienda a su presentación del Formulario 8-K conforme a este Punto 1.05 que contenga dicha información dentro de los cuatro días hábiles posteriores a la fecha en que el registrante, sin demora injustificada, determine dicha información o dentro de los cuatro días hábiles siguientes a la fecha en que dicha información esté disponible").

[[7]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref7%22%20%5Co%20%22) *Véase, por ejemplo*, 17 CFR 229.402(a)(2) (que exige "la divulgación de toda la remuneración otorgada y no relacionada con el plan, ganada o pagada a" ciertos funcionarios ejecutivos y directores).

[[8]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref8%22%20%5Co%20%22) *Véase*Adoption Release en 51899-900; Proponiendo la liberación en 16596.

[[9]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref9%22%20%5Co%20%22)  426 U.S. 438, 449 (1976).

[[10]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref10%22%20%5Co%20%22) 485 U.S. 224, 232 (1988).

[[11]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref11%22%20%5Co%20%22) 563 U.S. 27 (2011).

[[12]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref12%22%20%5Co%20%22) *Véase*17 CFR 230.405; 17 CFR 240.12b-2.

[[13]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref13%22%20%5Co%20%22) *Véase*Determinaciones de demora en incidentes de ciberseguridad material del Departamento de Justicia (12 de diciembre de 2023), *disponible en* <https://www.justice.gov/media/1328226/dl?inline>.

[[14]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref14%22%20%5Co%20%22) *Véase id*. en 2 ("Cuando un solicitante de registro descubre un incidente de ciberseguridad y cree que la divulgación puede representar un riesgo sustancial para la seguridad nacional o la seguridad pública, el solicitante de registro debe, directamente o a través de otra agencia del gobierno de los EE. UU. (por *ejemplo*, el Servicio Secreto de los EE. UU., otra agencia federal de aplicación de la ley, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) u otra agencia de gestión de riesgos sectoriales(SRMA)), ponerse en contacto inmediatamente con el FBI de acuerdo con las instrucciones de presentación de informes que el FBI ha emitido"). Las instrucciones de información del FBI están disponibles en <https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements>.

[[15]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref15%22%20%5Co%20%22) *Véase*el Formulario 8-K de Interpretación de Cumplimiento y Divulgación de la Ley del Mercado de Valores, preguntas 104B.01, 104B.02, 104B.03 y 104B.04, *disponibles en* [https://www.sec.gov/divisions/corpfin/guidance/8-kinterp.htm](https://www.sec.gov/divisions/corpfin/guidance/8-kinterp.htm#104b.01).

[[16]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref16%22%20%5Co%20%22) *Véase*la Instrucción 1 al punto 1.05 del Formulario 8-K ("La determinación de importancia relativa de un solicitante de registro con respecto a un incidente de ciberseguridad debe realizarse sin demora injustificada después del descubrimiento del incidente").

[[17]](https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214%22%20%5Cl%20%22_ftnref17%22%20%5Co%20%22) *Véase Pay Versus Performance*, Comunicado n.º 34-95607 (25 de agosto de 2022) [87 FR 55134 (8 de septiembre de 2022)].