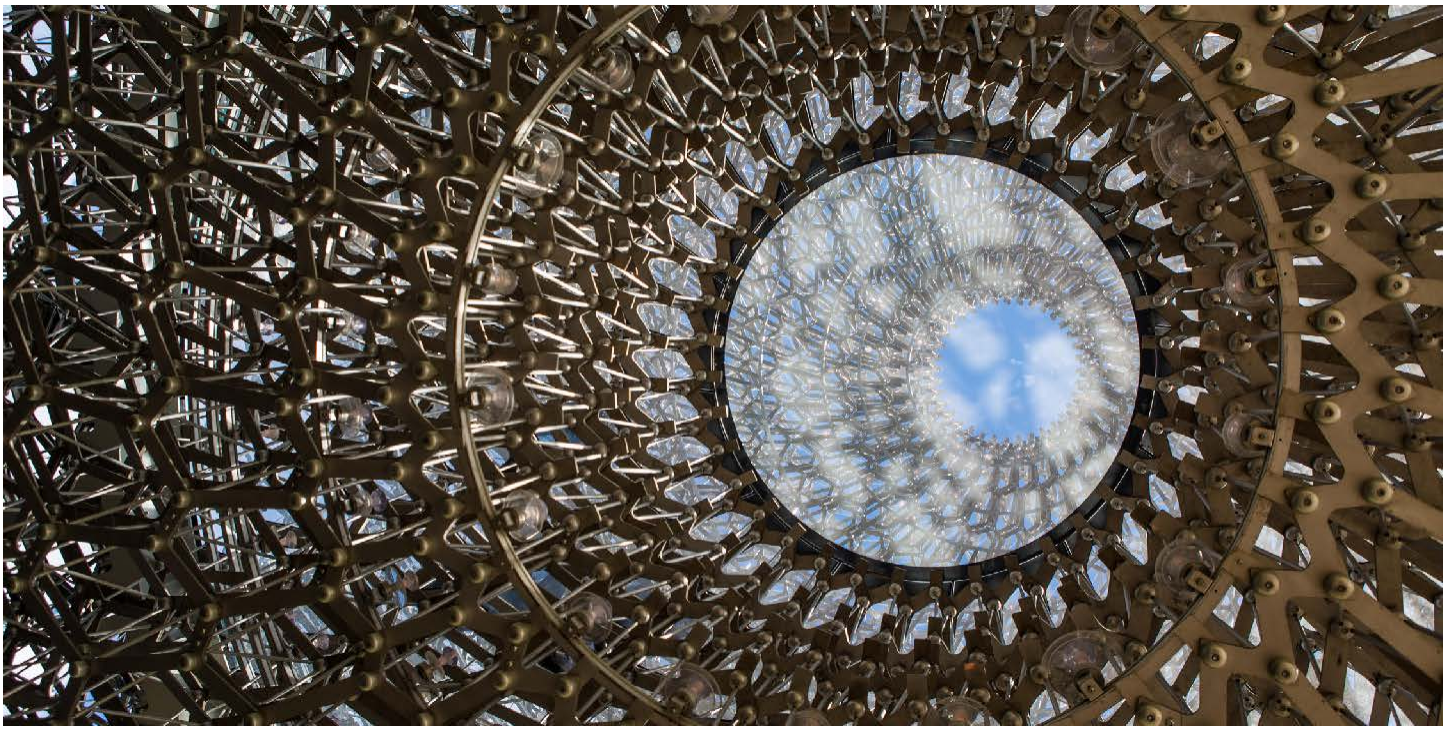
Deloitte.

Heads Up | Volume 25, No. 2
Febrero 23, 2018



En este número

"En el entorno de hoy, la seguridad cibernética es crítica para las operaciones de las compañías y de nuestros mercados."

— SEC Chairman Jay Clayton

En el espíritu de la revelación plena de la seguridad cibernética

Por Christine Mazor y Sandra Herrygers, Deloitte & Touche LLP

Antecedentes

En febrero 21, 2018, la SEC emitió orientación interpretativa (la "comunicación")[1] en respuesta al incremento generalizado en la tecnología digital, así como también la severidad y frecuencia de las amenazas e incidentes de seguridad cibernética. Esta comunicación refresca de manera amplia la orientación existente del personal de la SEC relacionada con la seguridad cibernética y, al igual que la orientación, no establece ninguna obligación nueva de revelación, sino que presenta los puntos de vista de la SEC sobre cómo sus reglas existentes deben ser interpretadas en conexión con las amenazas e incidentes de seguridad cibernética.

La comunicación se volverá efectiva en la fecha de su publicación en el *Federal Register*. En una declaración pública acerca de la comunicación, el SEC Chairman Jay Clayton observó que le solicitó a la Division of Corporation Finance que continúe monitoreando de manera cercana las revelaciones de la seguridad cibernética como parte de su proceso de revisión de registros y que la SEC continuará evaluando si se necesita orientación adicional. A la luz del centro de atención de la SEC puesto en materias de seguridad cibernética, las compañías pueden querer revisar sus revelaciones y sus controles y procedimientos de revelación ☐disclosure controls and procedures (DCPs)☐, incluyendo controles sobre las ventas de valores por parte de ejecutivos.

Los ataques cibernéticos pueden variar ampliamente de compañía a compañía. Pueden incluir el robo de activos financieros, propiedad intelectual, o información sensible de la compañía (o de sus clientes o proveedores), la disrupción de las operaciones de la compañía, o el objetivo de entidades que operan en industrias responsables por infraestructura crítica, tal como las industrias de energía y servicios públicos. Los costos y las consecuencias de un incidente de seguridad cibernética pueden incluir gastos de remediación, pérdida de ingresos ordinarios, litigios, primas de seguros incrementadas, daño reputacional, y erosión del valor de accionista.

[1] SEC Interpretative Release No. 33-10459, Commission Statement and Guidance on Public Company Cybersecurity Disclosures.

En el año 2011, la Division of Corporation Finance, de la SEC, emitió orientación[2] basada-en-principios que proporciona los puntos de vista de la SEC sobre las revelaciones de revelación de la seguridad cibernética, incluyendo las relacionadas con factores de riesgo, MD&A, y los estados financieros. La comunicación se extiende en los conceptos discutidos en esa orientación y se concentra más fuertemente en las políticas y controles de seguridad cibernética, principalmente en los relacionados con procedimientos de escalonamiento de la seguridad cibernética y la aplicación de prohibiciones de uso de información privilegiada. También aborda la importancia de evitar revelaciones selectivas, así como también la consideración del rol que la junta de directores tiene en la vigilancia del riesgo.

La comunicación aplica a las compañías de operación pública, incluyendo emisores privados extranjeros, pero no aborda las implicaciones específicas de la seguridad cibernética para otras entidades reguladas según las leyes federales de valores, tales como compañías de inversión registradas, asesores de inversión, corredores, distribuidores, bolsas de valores, y organizaciones auto-regulatorias.

Vista de conjunto de la orientación de la SEC sobre revelaciones y procedimientos de seguridad cibernética

La tabla que aparece a continuación proporciona una vista de conjunto de los puntos de vista sobre los requerimientos y procedimientos de revelación de la seguridad cibernética según las leyes federales de valores, tal y como están articulados en la comunicación. También muestra cómo la comunicación afecta la orientación del personal de la SEC emitida en 2011.

Tipo de revelación	Orientación contenida en la comunicación	Comparación con la orientación de 2011
Orientaciones generales de revelación	Proporciona orientación oportuna, actual, y adaptada en relación con los riesgos e incidentes materiales de seguridad cibernética contenidos en los registros SEC, incluyendo reportes corrientes y periódicos, así como también declaraciones de registro. Por ejemplo, si la compañía identifica un riesgo o incidente de seguridad cibernética que sería material para los inversionistas, debe revelar la información apropiada antes de cualquier oferta o venta de valores. La determinación de la materialidad[3] acerca de los riesgos e incidentes de seguridad cibernética depende de su naturaleza, extensión, y potencial magnitud así como también del daño que los incidentes podrían causar. La SEC observa que “las compañías en general sopesan, entre otras cosas, la potencial materialidad de cualquier riesgo identificado y, en el caso de incidentes, la importancia de cualquier información comprometida y del impacto del incidente en las operaciones de la compañía.” Las compañías deben considerar si necesitan revisar o refrescar su revelación anterior acerca de incidentes en la medida en que se desarrollen las investigaciones.	**Ampliada**

[2] CF Disclosure Guidance: Topic 2, “Cybersecurity.”

[3] La comunicación señala que la SEC considera que información omitida es material tal y como es articulado por la U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976) si (1) “Hay una probabilidad importante de que un inversionista razonable consideraría que la información es importante” al tomar una decisión de inversión, o (2) la revelación de la información “habría sido vista por el inversionista razonable como que de manera importante ha alterado la ‘mezcla total’ de información disponible.”

(Continúa la tabla)

Tipo de revelación	Orientación contenida en la comunicación	Comparación con la orientación de 2011
Factores de riesgo	Considere lo siguiente en la determinación de los riesgos a revelar en conexión con la seguridad cibernética y los incidentes relacionados: • Aspectos del negocio que estén sujetos a riesgos materiales de seguridad cibernética. • Lo adecuado y los costos de las medidas preventivas y de mitigación. • La frecuencia y severidad de incidentes pasados. • Probabilidad e importancia de incidentes futuros • Costos para proteger o remediar (o ambos), incluyendo seguros (si es aplicable). • Potencial para daño reputacional. • Requerimientos regulatorios y costos de cumplimientos. • Costos de litigios, investigación, y remediación. Para una compañía que tuvo una violación material previa de la seguridad cibernética puede no ser suficiente revelar que hay un riesgo de que podría ocurrir una violación. La compañía también necesita discutir el incidente de seguridad cibernética y sus consecuencias para proporcionar contexto para sus riesgos de seguridad cibernética.	**Consistente**
MD&A	Discuta los eventos, tendencias, o incertidumbres de seguridad cibernética que sea razonablemente probable tengan un efecto material en los resultados de las operaciones de la compañía, su liquidez, o condición financiera, incluyendo el impacto potencial en cada segmento reportable, si es aplicable. Considere la miríada de costos asociados con el evento de seguridad cibernética cuando evalúe la transparencia de las revelaciones de MD&A, incluyendo, pero no limitados a, los costos directos de los eventos, los costos asociados con la implementación de medidas preventivas, y el efecto de cualquier posible daño reputacional.	**Consistente**
Descripción del negocio	Proporcione revelación apropiada cuando cualesquiera riesgos o incidentes de seguridad cibernética afecten materialmente los productos de la compañía, sus servicios, relaciones con clientes o proveedores, o el entorno competitivo.	**Consistente**
Procedimientos legales	El requerimiento para revelar información relacionada con procedimientos legales materiales pendientes que involucren a la compañía o a sus subsidiarias también se extiende a los litigios relacionados con seguridad cibernética.	**Consistente**
Revelaciones del estado financiero	Los sistemas de presentación de reportes y control de la compañía deben estar diseñados para proporcionar seguridad razonable de que la información acerca del rango y magnitud de los efectos financieros de un incidente de seguridad cibernética serían incorporados en sus estados financieros sobre una base oportuna cuando la información esté disponible. Las revelaciones del estado financiero relacionadas con el impacto de incidentes materiales de seguridad cibernética pueden incluir, pero no están limitados a, información acerca de: • Costos materiales • Posibles cargos por deterioro • Ingresos ordinarios e incentivos de clientes • Reclamos u obligaciones por garantía • Causaciones por contingencias y litigios	**Consistente**

Vigilancia de la junta, sobre el riesgo[4]	Si los riesgos de seguridad cibernética son materiales para el negocio de la compañía, la discusión del rol que la junta de directores tiene en la función de vigilancia del riesgo debe incluir la naturaleza de sus responsabilidades por vigilar la administración de este riesgo. La SEC considera que “las revelaciones relacionadas con el programa de administración del riesgo de seguridad cibernética de la compañía y cómo la junta de directores se compromete con la administración en relación con los problemas de seguridad cibernética les permiten a los inversionistas valorar cómo la junta de directores está descargando su responsabilidad de vigilancia del riesgo en esta área crecientemente importante.”	**Nuevo**

Conectando los puntos

La SEC reconoció que no espera que las revelaciones de la compañía proporcionen un nivel de detalle que pudiera comprometer sus esfuerzos de seguridad cibernética y que en las primeras etapas de investigación de un incidente de seguridad cibernética puede haber disponible información limitada. Sin embargo, la SEC enfatizó que cuando la información está disponible, las entidades registradas son responsables por revelar información apropiada para mantener a los inversionistas informados y tienen que balancear la necesidad de revelación oportuna con el nivel de detalle que puedan proporcionar acerca de tales incidentes. Si bien la cooperación con el cumplimiento forzoso de la ley durante una investigación continua de un incidente material de seguridad cibernética puede ser necesaria y puede afectar el alcance de la revelación, ello solo no proporcionaría una base para omitir revelaciones materiales.

[4] SEC Regulation S-K, Item 407, “Corporate Governance.”

Políticas y procedimientos	Orientación contenida en la comunicación	Comparación con la orientación de 2011
DCP	Los DCP deben abordar la identificación y el escalonamiento del incidente de seguridad cibernética a los niveles apropiados dentro de la organización, lo cual incluiría asegurar que todas las partes relevantes, incluyendo las funciones de TI y negocios de la compañía, estén involucradas en la valoración del efecto potencial de la violación y los requerimientos relacionados de revelación. La revelación de manera importante amplía la orientación sobre la consideración de los DCP relacionados con los riesgos de seguridad cibernética. La SEC enfatizó que "las políticas y los procedimientos de administración del riesgo de seguridad cibernética son elementos clave de la administración del riesgo de toda la empresa, incluyendo en lo que se relaciona con el cumplimiento con las leyes federales de valores."	**Ampliado**
Revelaciones acerca de DCP[5]	Las certificaciones[6] del director ejecutivo principal y de los directores financieros principales, así como las revelaciones de la compañía en relación con el diseño y la efectividad de los DCP deben tener en cuenta lo adecuado de los controles y procedimientos para identificar y valorar el impacto de los riesgos e incidentes de seguridad cibernética. Si los riesgos o incidentes de seguridad cibernética dan origen a deficiencias en los DCP, las compañías deben tener ello en cuenta cuando revelen las conclusiones acerca de la efectividad de los DCP.	**Ampliado**
Uso de información privilegiada	Dado que los riesgos o incidentes de seguridad cibernética pueden constituir información no-pública material, las compañías deben considerar cómo sus códigos de ética y sus políticas de uso de información privilegiada abordan, previenen, y detectan el tráfico que se base en información material no-pública relacionada con seguridad cibernética. Las compañías también deben considerar si, y si es así, cuándo implementar restricciones al uso de información privilegiada cuando valoren e investiguen los incidentes de seguridad cibernética.	**Nuevo**
Regulación FD[7] y revelación selectiva	Las compañías deben asegurar que no violen la Regulation FD mediante selectivamente revelar información no-pública material relacionada con riesgos o incidentes de seguridad cibernética. Deben considerar las políticas y procedimientos apropiados para asegurar que los incidentes de seguridad cibernética no sean revelados selectivamente.	**Nuevo**

Otros Recursos

Como los pedidos para mayor transparencia relacionada con los riesgos de seguridad cibernética se han incrementado, recursos tales como los siguientes han sido desarrollados para ayudarles a las compañías tanto a valorar su enfoque frente a tal riesgo, como a considerar las revelaciones relacionadas:

- En el año 2017, el AICPA emitió una new cybersecurity risk management attestation reporting framework [nueva estructura para atestación y presentación de reportes sobre la administración del riesgo de seguridad cibernética] que tiene la intención de ayudarles a las organizaciones a evaluar y reportar sobre su programa de administración del riesgo de seguridad cibernética.

- La publicación de Deloitte, *The Value of Visibility: Cybersecurity Risk Management Examination* [El valor de la visibilidad: Examen de la administración del riesgo de seguridad cibernética], discute la estructura del AICPA y la preparación del enfoque de valoración para ayudar a las organizaciones a que preparen su respuesta al entorno actual de amenaza.

- La publicación de Deloitte, *Changing the Game on Cyber Risk: The Imperative to Be Secure, Vigilant, and Resilient* [Cambiando el juego del riesgo cibernético: El imperative de estar seguro, vigilante, y con capacidad de recuperación], aborda cómo las organizaciones pueden reversar la creciente brecha entre inversión en seguridad y efectividad de la seguridad.

[5] Requeridas por las Exchange Act Rules 13a-14 and 15d-14 and SEC Regulation S-K, Item 307, "Disclosure Controls and Procedures."

[6] La Sección 302 de la Sarbanes-Oxley Act of 2002 requirió que la SEC adopte reglas finales según las cuales el director (o directores) ejecutivo principal y el director (o directores) financiero principal, o las personas que proporcionen funciones similares, de un emisor tienen cada uno de ellos que certificar la información contenida en los reportes trimestral y anual del emisor.

[7] SEC Final Rule Release No. 33-7881, Selective Disclosure and Insider Trading (Regulation FD — Fair Disclosure).

Subscripciones

Si usted desea recibir *Heads Up* y otras publicaciones de contabilidad emitidas por el Accounting Standards and Communications Group, de Deloitte, por favor regístrese en www.deloitte.com/us/subscriptions.

D*briefs* para ejecutivos financieros

Lo invitamos a que participe en Dbriefs, la serie de webcast de Deloitte que entrega las estrategias prácticas que usted necesita para mantenerse en la cima de los problemas que son importantes. Tenga acceso a ideas valiosas e información crítica de los webcast en las series "Ejecutivos Financieros" sobre los siguientes temas:

- Estrategia de negocios e impuestos
- Perspectivas del controlador
- Orientando el valor de la empresa
- Información financiera
- Información financiera para impuestos
- Gobierno, riesgo y cumplimiento
- Contabilidad tributaria y provisiones
- Transacciones y eventos de negocio

Dbriefs también proporciona una manera conveniente y flexible para ganar créditos de CPE – directo en su escritorio. Suscríbase *Dbriefs* para recibir notificaciones sobre futuros webcast en www.deloitte.com/us/dbriefs

DART y US GAAP Plus

Tenga mucha información al alcance de su mano. La Deloitte Accounting Research Tool (DART) es una biblioteca comprensiva en línea de literatura sobre contabilidad y revelación financiera. Contiene material proveniente de FASB, EITF, AICPA, PCAOB, IASB y SEC, además de los manuales de contabilidad propios Deloitte y otra orientación interpretativa y publicaciones.

Actualizada cada día de negocios, DART tiene un diseño intuitivo y un sistema de navegación que, junto con sus poderosas características de búsqueda, les permite a los usuarios localizar rápidamente información en cualquier momento, desde cualquier dispositivo y buscador. Si bien buena parte del contenido de DART está contenido sin costo, los suscriptores pueden tener acceso a contenido Premium, tal como el FASB Accounting Standards Codification Manual [Manual de la codificación de los estándares de contabilidad de FASB], de Deloitte, y también pueden recibir *Technically Speaking*, la publicación semanal que resalta las adiciones recientes a DART. Para más información, o inscribirse para 30 días gratis de prueba del contenido Premium de DART, visite dart.deloitte.com.

Además, asegúrese de visitar US GAAP Plus, nuestro nuevo sitio web gratis que destaca noticias de contabilidad, información, y publicaciones con un centro de atención puesto en los US GAAP. Contiene artículos sobre las actividades de FASB y las de otros emisores de estándar y reguladores de Estados Unidos e internacional, tales como PCAOB, AICPA, SEC, IASB y el IFRS Interpretations Committee. ¡Dele un vistazo hoy!

Esta es una traducción al español de la versión oficial en inglés de **Heads Up – Volume 25, Issue 2 – February 23, 2018 – In the Spirit of Full Cybersecurity Disclosure –** Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia.