Spread the love

La gestión de la seguridad cibernética se percibe, cada vez más, como parte integrante de las medidas de buen gobierno exigidas a las empresas.

Venimos dando cuenta en este Blog, y en algunos otros foros, de la creciente relevancia de los riesgos cibernéticos en el diseño, valoración y en su caso, sanciones (ver esta entrada), en materia de gobierno corporativo. Los asuntos que aquí se presentan brevemente *son objeto de atención en modo más amplio en el contexto del Congreso Latinoamericano INTELIGENCIA ARTIFICIAL Y ECONOMÍA DIGITAL: desafíos jurídicos y económicos* (13 al 15 octubre 2021) y en una publicación ya en imprenta de la que se dará cuenta.

Guías, orientaciones y previsiones normativas del Regulador de Valores de EEUU en relación con la ciberseguridad

Regulación prevista

Conforme a la Agenda Regulatoria de primavera de 2021 de la SEC, el Supervisor de Valores de EEUU está en vías de formular nuevas reglas que afectarán de lleno a las obligaciones de gobierno corporativo de las empresas y en concreto, a la divulgación de riesgos de seguridad cibernética. Se prevé que las mencionadas propuestas vean formalmente la luz en octubre de 2021. Estos trabajos toman base en las Orientaciones sobre Ciberseguridad de la SEC (febrero 2018) en las que ya se vinculaba el cumplimiento de distintas obligaciones de transparencia sobre riesgos de ciberseguridad con el buen gobierno. Incluso antes, en 2011 la División de Finanzas Corporativas de la SEC había publicado una Guía preliminarsobre estas cuestiones.

La Agenda ReEgFlez mencionada, ya apunta a octubre de 2021 como la fecha límite para la emisión de una propuesta. (Vea esta publicación de PubCo de 14.06.2021). En el actual entorno en el que se conoce la abundancia y dureza de ataques cibernéticos y la posibilidad de infección por ransomware, es más que posible que la SEC pueda proponer enmiendas a

sus Rules de transparencia para mejorar las divulgaciones de los emisores con respecto a la gobernanza del riesgo de ciberseguridad.

Sanabria

Antecedentes. La Guía de la SEC de 2018 sobre divulgación de informaciones relativas a la seguridad cibernética

Con anterioridad, la Guía de la SEC de 2018 sobre divulgación de seguridad cibernética abordó las obligaciones de divulgación al amparo del ordenamiento vigente, que incluía procedimientos, políticas y estrategias para el control de la seguridad, entendida en un sentido amplio, prohibiciones de aprovechar información privilegiada, o de difundir datos selectivamente, entre otros.

- La Guía mencionada señala que *los incidentes de ciberseguridad pueden ser el resultado de eventos no intencionales, pero también de ataques deliberados, y que pueden ser realizados por personas con información privilegiada, o por terceros.*
- Con respecto a las **políticas, controles y procedimientos de ciberseguridad**, la SEC alentó en 2018 a las empresas a adoptar y evaluar periódicamente el cumplimiento de políticas y procedimientos integrales relacionados con la ciberseguridad, en particular con los controles y procedimientos de divulgación. Además, instaba a las empresas a evaluar si sus controles y procedimientos de divulgación eran suficientemente precisos y adecuados como para localizar información sobre los riesgos e incidentes de ciberseguridad, y también para difundir el conocimiento de esos riesgos entre la alta jerarquía corporativa para permitir que la alta dirección adopte decisiones.
    - Conforme a la Guía mencionada (de 2018), los controles y procedimientos corporativos deben permitir a las empresas identificar los riesgos e incidentes de ciberseguridad, evaluar y analizar su impacto en el negocio de una empresa, evaluar la importancia asociada con dichos riesgos e incidentes, proporcionar comunicaciones abiertas entre expertos técnicos y asesores de divulgación. Deben ser adecuadas para realizar divulgaciones oportunas sobre dichos riesgos e incidentes.
    - Los controles también deben permitir que la información se comunique al

personal correspondiente, para facilitar el cumplimiento de las políticas de uso de información privilegiada.

- Por otro lado, y ya de lleno en consideraciones propias del Gobierno Corporativo clásico (y de las obligaciones de transparencia relacionadas), dado que las notificaciones que los principales ejecutivos, el CEO y el CFO están obligados a emitir en sus informes periódicos al supervisor abordan la efectividad de los controles corporativos, la SEC adelantaba en su Guía de 2018 que estas certificaciones deberían tener en cuenta la idoneidad de los controles y procedimientos para identificar los riesgos e incidentes de ciberseguridad.
- Con respecto a la divulgación, la Guía de 2018 ya señalaba que incluso en ausencia de exigencias de divulgación especificadas normativamente en relación con los riesgos e incidentes de ciberseguridad:
    - La obligación de divulgar tales riesgos se entendería implícita -dependiendo de las circunstancias particulares de cada entidad- en el conjunto de obligaciones de transparencia (declaraciones ante la SEC, informes periódicos, informes anuales, etc.).
    - Conforme a la Regla 10b-5 (y disposiciones similares) las entidades sometidas a la supervisión de la SEC están obligadas a valorar si sus divulgaciones proporcionan todos los *hechos materiales*, y en ese sentido, incluir en ellas las cuestiones relativas a ciberseguridad que deban considerarse «**materiales**» para evitar que el conjunto de la declaración resulte engañosa. En ese sentido, el Supervisor estadounidense alentó a las empresas a utilizar el Formulario 8-K para informar al supervisor y al mercado también sobre los costos y otras consecuencias de los incidentes materiales de ciberseguridad.

        - En relación con esta Guía y con los futuros desarrollo que se produzcan en torno a la obligación de comunicar riesgos e incidentes cibernéticos, debemos llamar la atención sobre la dificultad de determinar si la divulgación sobre los riesgos e incidentes de ciberseguridad es necesaria. En este sentido, el Supervisor de mercados estadounidense recordaba que las empresas generalmente sopesan, entre otras cosas, **la materialidad potencial** de cualquier riesgo identificado. Pues bien, en el caso de incidentes cibernético, la valoración de si resultan «materiales» debe realizarse a la luz de la importancia de la información comprometida, propiamente dicha, y también del impacto (actual o probable) del incidente sobre las operaciones de la empresa. Y, este ejercicio, que se realiza ya en otros

ámbitos que son susceptibles de generar riesgos y que ya son objeto de comunicación al Supervisor, ha de contemplarse también en el ámbito de los riesgos cibernéticos.

- La SEC señaló que el *caso Basic v. Levinson*, en el que se articuló la teoría jurisprudencial de «fraude al mercado» y que sirve de pauta sobre la probabilidad de que se deriven daños relevantes, sigue siendo una parte relevante del análisis. Debe recordarse que en esta importante sentencia federal se revisaron los estándares de **materiality**, tomando en cuenta otra decisión previa (especialmente la de *TSC Industries, Inc. v. Northway, Inc.*, que señala que en relación con la transparencia exigida a las empresas supervisadas «un hecho es material si existe una probabilidad sustancial de que un accionista «razonable» lo consideraría importante a la hora de decidir su voto» , pauta que se viene utilizando como referencia para el cumplimiento y la supervisión de las obligaciones de transparencia derivadas del artículo § 10(b) de la *Securities Exchange Act* y la *Rule 10b-5* de la SEC.
- La SEC también advirtió que la importancia relativa de los riesgos o incidentes de seguridad cibernética depende de su naturaleza, alcance y magnitud potencial, particularmente en lo que respecta a cualquier información comprometida para la actividad de la entidad o para sus operaciones. En ese sentido, la SEC subrayó que la información comprometida «podría incluir información de identificación personal, secretos comerciales u otra información comercial confidencial, cuya ***materialidad*** puede depender de la naturaleza del negocio, así como del alcance de la información comprometida». Y, que la materialidad "también depende del rango de daño o daños que los incidentes sean susceptibles de causar», y que abarcan desde daños reputacionales, daños financieros, hasta otros derivados de las relaciones con los clientes y proveedores y con el incremento en la posibilidad de litigios, investigaciones o de que la

empresa vaya a quedar sometida a investigaciones (o sanciones) por parte de las autoridades.

Como ya es conocido en otros ámbitos, la SEC advirtió a las empresas que «eviten la divulgación genérica» (ahora relacionada con la ciberseguridad) y les instó a que proporcionen información específica que sea útil para los inversores.

Aunque se espera que las empresas «revelen los riesgos e incidentes de ciberseguridad que son importantes para los inversores, incluidas las consecuencias financieras, legales o de reputación concomitantes», la SEC dejó en claro que no se espera que proporcionen detalles o información técnica específica sobre posibles vulnerabilidades del sistema que puedan comprometer la seguridad del emisor.

Para obtener más información sobre la guía de la SEC, consulten esta publicación de PubCo (18 febrero 2018) y esta alerta de Cooley .

Comunicaciones con el sector financiero sobre la necesidad de mayor transparencia de riesgos cibernéticos

Ox

A fines de 2018, según lo informado el 13.11.2018 por el *WSJ* , el entonces Chief accountant de la Securities and Exchange Commission's Corporation Finance Division, , Kyle Moffatt, en su intervención en la importantísima conferencia sectorial, FEI, «Current Financial Reporting Issues Conference», instó a las empresas a alinear sus prácticas de divulgación con la guía de divulgación de ciberseguridad de la SEC, citando en particular la necesidad de abordar un debate de calado sobre riesgos de supervisión, el papel de la junta, los controles y los procedimientos internos de divulgación de datos e informaciones y las políticas de uso de información privilegiada en el contexto de la ciberseguridad. Además, advirtió que "la clave más importante es asegurarse de que existan procedimientos para asegurarse de que la información se brinde a todos los niveles de la gestión empresarial, para que todos estén al tanto de lo que sucedió y para que los problemas se pueden abordar. '"(Consulte esta publicación de PubCo de 14 noviembre 2014).

Estas declaraciones son, no sólo sintomáticas, sino que reflejan en buena medida la posición

del sector.