ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

Los ciberataques en la empresa cotizada y su impacto en el valor de las acciones

FRANCISCO PERÉZ BES

POLICY BRIEF
Marzo 2023

POLICY BRIEF

Los ciberataques en la empresa cotizada y su impacto en el valor de las acciones

Contacto

Calle de Caracas, 6, Planta Baja, 28010, Madrid.

+34 914252577 /609484940
www.fundacionesys.com

FRANCISCO PERÉZ BES

Francisco Pérez Bes. Abogado. Socio de Derecho Digital en Ecix. Antiguo Secretario General del Instituto Nacional de Ciberseguridad de España (INCIBE). Embajador de la National CyberLeague de la Guardia Civil. Autor del Código Electrónico BOE de Derecho de la Ciberseguridad.

Marzo 2023

POLICY BRIEF

Resumen

En el entorno de las empresas cotizadas, el impacto de los ciberataques va más allá de los meros aspectos técnicos o de protección de datos, y se adentra en obligaciones de naturaleza económica y de regulación del mercado. En este escenario, cobra especial relevancia la implementación de medidas técnicas y organizativas que permitan acreditar un alto nivel de diligencia a la hora de prevenir y gestionar los incidentes de seguridad, especialmente ante el riesgo del insider trading, además de la necesidad de delimitar cuál puede ser la responsabilidad de los Consejos de administración ante este tipo de situaciones. Todo ello, además, en un escenario de indeterminación tras la reciente publicación de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, la cual traspone la conocida como "Directiva de Whistleblowing", la cual recoge expresamente los incumplimientos de las regulaciones derivadas de la Directiva NIS[1].

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

[1] https://www.boe.es/doue/2019/305/L00017-00056.pdf

Marzo 2023

POLICY BRIEF

INTRODUCCIÓN

El artículo 10 de la Ley de Seguridad Nacional 36/2015 califica a la ciberseguridad y, en particular, a la seguridad económica y financiera, como dos ámbitos de especial interés para la Seguridad Nacional. En consecuencia, ambos aspectos requieren de una atención específica por resultar básicos para preservar los derechos y libertades, el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales.

Dentro de este escenario y con respecto a empresas de especial entidad o relevancia (bien sea por tamaño, tipo de actividad, carácter estratégico o similares), debemos destacar algunos aspectos relativos a la regulación de los incidentes de ciberseguridad que puedan afectar a tales organizaciones, como son, en particular, lo que se refiere a la normativa sobre protección de datos personales y a la de seguridad de las redes y sistemas de información.

En cuanto al Reglamento General de Protección de Datos, que -como es sabido- resulta exigible a cualquier tipo de organización con independencia de su tamaño y actividad, su régimen es aplicable siempre que el incidente de seguridad afecte a datos de carácter personal. La obligación contemplada en los artículos 5, 32 y siguientes del RGPD se centra en, principalmente, la exigencia de implementar medidas técnicas y organizativas, que deben ir dirigidas a la prevención, a la reacción (en particular la minimización del impacto negativo causado por el incidente una

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

vez se haya producido), y a la notificación del incidente en determinados supuestos (tanto al regulador como, en su caso, a los afectados).

De otro lado, el régimen regulado en la Directiva de Seguridad de las Redes y Sistemas de Información (comúnmente conocida como Directiva NIS), fue traspuesta al ordenamiento jurídico nacional a través del Real Decreto Ley 12/2018 y su Reglamento de desarrollo, aprobado mediante Real Decreto 43/2021. Esta regulación ha sido sustituida por la nueva Directiva 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (conocida como NIS2), publicada en el DOUE de 27 de diciembre de 2022.

Junto a aquella, ese mismo día se publicó la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE, y que aplica a lo que la norma denomina "entidades críticas" (en España, y hasta que se formalice la transposición de la Directiva, todavía sometidas a la regulación de la ley 8/2011 sobre protección de infraestructuras críticas y a su reglamento de desarrollo), entre las cuales es habitual que se encuentren empresas cotizadas, tanto en el IBEX 35 como en el mercado secundario.

Marzo 2023

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

ANTECEDENTES DE IMPACTO DE CIBERATAQUE EN LA COTIZACIÓN DE EMPRESAS ESPAÑOLAS

En 2020, la compañía aseguradora Mapfre hizo público haber sido víctima de un ciberataque, que -según afirmaron- afectó a sus sistemas informáticos de forma muy relevante. La rápida actuación de la empresa permitió reducir el impacto negativo del incidente, tanto dentro de la propia organización, como con respecto a terceros. Este elevado nivel de diligencia en su actuar les hizo merecedores, incluso, del reconocimiento del regulador español de protección de datos en la resolución que archivó la investigación iniciada.

Sin embargo, a pesar de ello, el nivel de confianza del mercado en la gestión de la compañía aparentemente se redujo. Tal y como reflejan algunas informaciones, durante los días siguientes, las acciones de Mapfre disminuyeron su valor de cotización entre un 1% y un 6%, reflejando una tendencia bajista superior a la del mercado, sin encontrar una explicación distinta de la del propio ciberataque[2].

A pesar de ello, el informe de auditoría de las Cuentas Anuales de la empresa (individual 2020) sólo hizo referencia al ciberataque dentro del apartado de “otros riesgos”, limitándose a afirmar que:

> *Durante el mes de agosto de 2020, MAPFRE detectó un malfuncionamiento en sus sistemas informáticos por un Ciberataque. Siguiendo los procedimientos establecidos, los equipos de tecnología y de seguridad iniciaron una investigación detectando que un malware, en particular un ransomware, había logrado infiltrarse en sus sistemas informáticos, que afectaba a parte de los servidores y equipos en España.*
>
> *Desde el primer momento, se activaron los protocolos previstos en el plan de continuidad de negocio, siendo la prioridad proteger la información y bloquear todo posible intento de acceso de terceros a los sistemas, así como garantizar la prestación del servicio a clientes y proveedores que se mantuvo en todo momento gracias a los procedimientos alternativos previstos.*

[2] https://cso.computerworld.es/cibercrimen/retroceso-de-mapfre-en-bolsa-tras-el-ciberataque

Esta anormal alteración de la cotización de las acciones una vez la empresa ha sufrido el impacto de un incidente de ciberseguridad de cierta entidad, **puede llevarnos a concluir que un ciberataque podría tener la capacidad de afectar negativamente al valor de las acciones de una empresa. ¿Podríamos, por tanto, estar ante una herramienta idónea para manipular su cotización?**

Antes de intentar responder a esta pregunta, conviene analizar qué empresas del IBEX-35 han reconocido públicamente, a fecha de elaboración de este análisis, haber sufrido un incidente de seguridad que pueda ser calificado como ciberataque. En particular, las referencias públicas a las que se han podido tener acceso han sido:

Empresa del IBEX	Fecha del incidente	Tipología de incidente
Banco de Santander	Mayo de 2017	No declarado [3]
Endesa	Octubre de 2020	Ransomware [4]
IAG (filial UK)	2018	Robo de datos [5]
Iberdrola	Marzo de 2022	Robo de datos [6]
Indra	Diciembre de 2017	Ataque [7]
Mapfre	Agosto de 2020	Ransomware [8]
Meliá	Octubre de 2021	Ransomware [9]
Naturgy	Diciembre de 2018	Robo de datos [10]
Telefónica	Mayo de 2017	Ransomware (WannaCry) [11]

Fuente: elaboración propia

[3]https://www.expansion.com/juridico/actualidad-tendencias/2021/04/16/60797e38468aeb0e558b4582.html

[4]https://elpais.com/tecnologia/2020-10-20/endesa-asegura-haber-resistido-sin-consecuencias-un-ataque-informatico.html

[5] https://www.ccn-cert.cni.es/ca/gestion-de-incidentes/lucia/23-noticias/7103-185-000-clientes-de-british-airways-victimas-de-un-ciberataque-segun-iag.html

[6] https://www.osi.es/es/actualidad/avisos/2022/03/iberdrola-comunica-sus-clientes-que-ha-sido-victima-de-un-ciberataque

[7] https://elpais.com/economia/2017/12/13/actualidad/1513170207_034592.html

[8]https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/mapfre-sufre-ciberataque-ransomware

[9]https://www.europapress.es/turismo/hoteles/noticia-melia-sufre-ciberataque-afecta-varios-hoteles-grupo-20211004201209.html

[10]https://www.elconfidencial.com/empresas/2019-07-18/naturgy-chantaje-robo-informacion-confidencial-ciberataque_2130979/

[11] https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/telefonica-afectada-ransomware

SOBRE LA ALTERACIÓN DE PRECIOS DEL MERCADO

Si un incidente de ciberseguridad intencionado puede alterar artificialmente los precios de las acciones de la empresa afectada, no cabe duda de que un ciberataque puede considerarse como un medio apto para manipular su cotización y, en consecuencia, afectar al normal comportamiento del propio mercado.

Ante tal posibilidad, la Ley Orgánica 1/2019, de 20 de febrero, al transponer al Derecho nacional la normativa europea sobre el abuso de mercado, modificó el artículo 284 del Código Penal para tipificar como delito de resultado lesivo aquellas prácticas que puedan resultar idóneas para alterar los precios de las acciones, afectar a la integridad de los mercados y perjudicar la confianza de los inversores que actúan en ellos. La nueva ley también modificó el artículo 285 del Código Penal para sancionar el uso ilícito de información privilegiada, lo que, como veremos, es una práctica que también puede concurrir en un caso como el que ahora nos ocupa.

A través de estos delitos, que se enmarcan en los Considerados de dicha ley como de naturaleza socioeconómica, se pretende sancionar los comportamientos que efectivamente atentan contra los precios de mercado que, por su gravedad, no pueden dejarse en el ámbito de la sanción administrativa del regulador competente (en este caso, la Comisión Nacional del Mercado de Valores).

En este tipo de situaciones, lo relevante a efectos de su tipicidad tiene que ver con si se ha producido una manipulación del mercado que haya tenido influencia en la adecuada formación de la cotización de los instrumentos financieros, perturbando así la integridad de los mercados de capitales.

Adicionalmente, debe tenerse en cuenta que ambos delitos forman parte de aquellos de los que puede derivarse responsabilidad penal de la persona jurídica, tal y como menciona el artículo 31 bis del Código Penal cuando pasa a regular lo que es comúnmente conocido como compliance penal.

EL INCIDENTE DE CIBERSEGURIDAD COMO ABUSO DE INFORMACIÓN PRIVILEGIADA: EL CASO DEL INSIDER TRADING

Algunos expertos han alertado de que la mera detección de determinadas brechas de seguridad en empresas cotizadas (en función de su gravedad y alcance), pueden ser calificadas como información privilegiada y, como tal, sujetas a las obligaciones de publicidad que establece el Reglamento de Abuso de Mercado de la Unión Europea. Esto se debe a que se puede considerar a los ciberataques como a hechos que conciernen directamente al emisor y que pueden llegar a influir de manera sustancial sobre los precios de las acciones o de los instrumentos financieros relacionados con las mismas[12].

Como indicábamos anteriormente, la citada reforma del Código Penal de 2019 endureció las penas por la utilización de información privilegiada (comúnmente conocida como insider trading), a la que describe como aquella actividad mediante la cual una persona es conocedora de que se va a llevar a cabo una operación societaria y se aprovecha de tal conocimiento para lucrarse o para manipular el normal comportamiento del mercado.

Con relación a este tipo de prácticas ilícitas, el artículo 284.1 del Código Penal castiga con penas de prisión de hasta 6 años, multa e inhabilitación, a los que:

> *Empleando violencia, amenaza, engaño o cualquier otro artificio, alterasen los precios que hubieren de resultar de la libre concurrencia de productos, mercancías, instrumentos financieros, contratos de contado sobre materias primas relacionadas con ellos, índices de referencia, servicios o cualesquiera otras cosas muebles o inmuebles que sean objeto de contratación, sin perjuicio de la pena que pudiere corresponderles por otros delitos cometidos.*

[12]https://www.eleconomista.es/legislacion/noticias/11423805/10/21/La-auditoria-externa-ya-incluye-la-ciberseguridad-como-riesgo-inversor.html

Mientras que el artículo 285.1 del Código Penal, sanciona el delito de uso ilícito de información privilegiada de la siguiente manera:

> *Quien de forma directa o indirecta o por persona interpuesta realizare actos de adquisición, transmisión o cesión de un instrumento financiero, o de cancelación o modificación de una orden relativa a un instrumento financiero, utilizando información privilegiada a la que hubiera tenido acceso reservado en los términos del apartado 4, o recomendare a un tercero el uso de dicha información privilegiada para alguno de esos actos, será castigado con la pena de prisión de seis meses a seis años, multa de dos a cinco años, o del tanto al triplo del beneficio obtenido o favorecido o de los perjuicios evitados si la cantidad resultante fuese más elevada, e inhabilitación especial para el ejercicio de la profesión o actividad de dos a cinco años, siempre que concurra alguna de las siguientes circunstancias*

A nuestro entender, este tipo de situaciones también pueden vincularse a aquellos casos en los que se produce un incidente de ciberseguridad en el seno de una corporación. En tal caso, podemos afirmar que una práctica de esta naturaleza puede ser considerada ilícita por cuanto resulta idónea para que una persona tenga conocimiento de la producción del incidente y de los detalles del mismo (lo que podemos calificar como de ”información privilegiada”), y se aproveche de la misma en el sentido de desprenderse de su participación accionarial en la empresa víctima del ciberataque (o de advertir a otros para que lo hagan), con carácter previo al conocimiento de la existencia de tal incidente por parte del regulador y del mercado y, por tanto, antes de que las acciones de la compañía afectada puedan ver reducido su precio de cotización. De tal manera que, una vez efectivamente se produzca esta eventual disminución del valor de las acciones, dicha persona logre un beneficio económico determinado, evite una pérdida, o un incremento de su participación accionarial en la empresa.

Ante un riesgo de esta naturaleza, la normativa española que regula los mercados financieros impone la obligación de comunicar al regulador cualquier tipo de incidente relevante que pueda afectar a los accionistas de la empresa afectada y, en consecuencia, al mercado en general.

En este caso, la Ley de Mercado de Valores regula este tipo de situaciones en su artículo 226, cuyo tenor literal es el siguiente:

> *Los emisores de valores o instrumentos financieros que sean objeto de negociación en un mercado regulado español, o respecto de los que haya sido solicitada la admisión a negociación, deberán comunicar tan pronto como sea posible a la CNMV, que procederá a hacerla pública en su página web, la información privilegiada que le concierna directamente a que se refiere el artículo 17 del Reglamento (UE) n.º 596/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014.*

En este sentido, cabe añadir que también Europa se ha hecho eco de este riesgo. En efecto, el Dictamen del Comité Económico y Social Europeo sobre la nueva Estrategia de Ciberseguridad europea[13], incluye, dentro de las pérdidas económicas derivadas de los ciberataques, a "la manipulación financiera, utilizando información empresarial sensible robada sobre posibles fusiones o conocimiento previo de informes de resultado de empresas cotizadas".

Por su parte, también encontramos precedentes de situaciones similares en Estados Unidos, donde su organismo regulador (la Security Exchange Commission, comúnmente conocida como SEC) ya ha investigado alguna controversia relacionada con este tipo de actividades ilícitas por parte de directivos de compañías tenedores de acciones de la empresa, que se desprenden de aquellas al conocer en primicia la producción de incidente de ciberseguridad con un impacto significativo, en la certeza de que el ciberataque provocará una bajada inmediata del precio de tales acciones, obteniendo el correspondiente beneficio.

Debemos remontarnos a 1995 para encontrar uno de los primeros casos relacionados con este tipo de prácticas, cuando el CEO de Intel vendió la mayoría de las acciones que poseía de la empresa tras descubrir que los procesadores que fabricaban tenían una vulnerabilidad crítica en su diseño, todo ello meses antes de que esta situación saltase a la prensa.

Más recientemente, uno de los casos más destacables es el que se refiere a las actividades del antiguo CIO de la empresa Equifax, Jun Ying, quien se desprendió de acciones de la compañía (stock options) por valor de casi un millón de dólares

[13] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.C_.2021.286.01.0076.01.SPA&toc=OJ%3AC%3A2021%3A286%3ATOC

una semana antes de que Equifax hiciera público el hackeo de su base de datos en septiembre de 2017, lo que le permitió obtener un beneficio de 480.000 dólares a la vista de que el precio de la acción de Equifax se desplomó un 30% tras revelarse públicamente la masiva brecha de seguridad sufrida por la compañía[14].

EL RÉGIMEN DE LA RESPONSABILIDAD DE LOS ADMINISTRADORES EN LA GESTIÓN DE CIBERINCIDENTES

Derivado de las anteriores cuestiones, es preciso analizar cuál es el nivel de responsabilidad de los órganos de administración de las compañías que son víctimas de ciberataques relevantes.

Para ello, debemos atender a lo que dispone la Ley de Sociedades de Capital (LSC) cuando recoge, como obligaciones de los administradores, la obligación de diligencia y la de lealtad.

A)EL DEBER DE DILIGENCIA Y LA CIBERSEGURIDAD

El deber de diligencia del administrador se recoge en el artículo 225.1 de la LSC con relación al estándar de conducta del ordenado empresario, teniendo en cuenta la naturaleza del cargo y las funciones atribuidas a cada administrador.

Además, ese mismo artículo añade obligaciones concretas relacionadas con la gestión de las actividades de la empresa, como son: (i) tener la dedicación adecuada; (ii) adoptar las medidas precisas para la buena dirección y el control de la sociedad; y (iii) tener conocimiento de la propia compañía, en el sentido de reconocerle el deber de exigir y el derecho de recabar de la sociedad la información adecuada y necesaria para el cumplimiento de sus obligaciones.

Entre tal información debería incluirse la relativa a la seguridad de la información y de las redes y sistemas de información donde se aloja, tal y como prevé el artículo 225.3 LSC.

[14] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355978

Ahora bien, no es menos cierto que **para poder garantizar que los administradores y consejeros de sociedades disponen de un conocimiento suficiente o adecuado de los riesgos de ciberseguridad que amenazan al negocio**, así como de sus consecuencias en la empresa o en el mercado, **el artículo 20.2 de la Directiva NIS2 prevé la obligación de formación en ciberseguridad a los directivos de la compañía:**

> *Los Estados miembros garantizarán que los miembros de los órganos de dirección de las entidades esenciales e importantes deban asistir a formaciones y alentarán a estas entidades para que ofrezcan formaciones similares a sus empleados periódicamente al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.*

No obstante, cabe recordar también que, en el derecho mercantil español, el deber de diligencia del administrador no constituye una obligación de resultado, sino -en líneas generales- de medios, dado que todo negocio conlleva un riesgo y este riesgo es parte del beneficio o pérdida que se genera para la sociedad. Esta aseveración va en consonancia con lo considerado por la sala Tercera del Tribunal Supremo con respecto a la protección de datos en su Sentencia de 15 de febrero de 2022, lo que podemos hacer extensivo a las obligaciones de ciberseguridad por cuanto la terminología empleada en esta normativa (caso, por ejemplo, del Real Decreto Ley 12/2018 y su normativa de desarrollo RD 43/2021) es idéntica a la utilizada por el Reglamento General de Protección de Datos cuando, en su artículo 32, obliga a implementar medidas técnicas y de organización adecuadas[15].

En efecto, el Alto Tribunal se expresa a este respecto afirmando que en las obligaciones de medios el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia " o "de comportamiento".

La diferencia entre ambos supuestos radica, a juicio del Tribunal Supremo español, *en la*

[15] Sentencia núm. 188/2022: https://www.poderjudicial.es/search/openDocument/28c1859e0a8c5444

responsabilidad en uno y otro caso, pues mientras que en la obligación de resultado se responde ante un resultado lesivo por el fallo del sistema de seguridad, cualquiera que sea su causa y la diligencia utilizada. En la obligación de medios basta con establecer medidas técnicamente adecuadas e implantarlas y utilizarlas con una diligencia razonable.

Sin embargo, no debemos dejar de destacar que el Tribunal Supremo no sólo se limita a interpretar la norma en el sentido de reconocer un deber de disponer de tales medidas, sino de que las mismas resulten eficaces para gestionar el riesgo al que se enfrenta la organización. Por tal motivo la citada sentencia añade que:

> *No basta con diseñar los medios técnicos y organizativos necesarios también es necesaria su correcta implantación y su utilización de forma apropiada, de modo que también responderá por la falta de la diligencia en su utilización, entendida como una diligencia razonable atendiendo a las circunstancias del caso.*

Adicionalmente, en el ámbito que ahora nos interesa, el Código de buen gobierno de las sociedades cotizadas (en su versión revisada en junio 2020) no hace ninguna mención ni referencia expresa a la ciberseguridad, si bien establece unas recomendaciones sobre los riesgos e información no financiera que pueden ser de interés con relación al supuesto que aquí nos ocupa. Y si bien su ámbito de aplicación se refiere a las sociedades cotizadas, puede servir de pauta para el resto de las empresas.

B)EL DEBER DE LEALTAD PARA CON LA EMPRESA

De conformidad con lo dispuesto en el artículo 227 de la LSC, los administradores deberán desempeñar el cargo con la lealtad de un fiel representante, obrando de buena fe y en el mejor interés de la sociedad. Esto es, que el deber de lealtad del administrador le exige anteponer en todo momento el interés social a cualquier otro interés, particularmente el interés propio.

Con tal de poder lograr dichos objetivos, los artículos 228 y 229 describen una serie de situaciones en las que el administrador debe evitar participar, entre las cuales podemos

sencontrar el uso de información privilegiada para cometer insider trading.

Por ejemplo, la obligación de guardar secreto sobre las informaciones, datos, informes o antecedentes a los que haya tenido acceso en el desempeño de su cargo, incluso cuando haya cesado en él, salvo en los casos en que la ley lo permita o requiera (228.b). O la obligación de adoptar las medidas necesarias para evitar incurrir en situaciones en las que sus intereses, sean por cuenta propia o ajena, puedan entrar en conflicto con el interés social y con sus deberes para con la sociedad (228.e). O el deber de abstenerse de hacer uso de los activos sociales, incluida la información confidencial de la compañía, con fines privados (229.c).

CONCLUSIONES

1. El impacto de un incidente de ciberseguridad puede afectar al valor de cotización de las acciones de la empresa afectada.

2. La información sobre incidentes de especial relevancia o con impacto significativo en la compañía, puede ser considerada información privilegiada.

3. La normativa sobre seguridad de la información y de las redes y sistemas (RGPD, NIS2, etc.) establece obligaciones claras de notificar los incidentes de seguridad a las autoridades competentes.

4. Determinadas personas de la empresa, o relacionada con ella, que tengan participación accionarial en aquella, pueden tener información privilegiada derivada de un incidente de ciberseguridad.

5. El delito de *insider trading* y de abuso de información privilegiada también incluye responsabilidad de la persona jurídica, lo que obliga a diseñar sistemas de prevención eficaces.

6. Es responsabilidad de los administradores adoptar medidas técnicas y organizativas preventivas y reactivas para evitar que puedan ocurrir este tipo de situaciones en el seno de su empresa, especialmente en las cotizadas.

7. Las normas de buen gobierno de las sociedades cotizadas deben actualizarse con tal de incluir referencias a los efectos de los incidentes de ciberseguridad y sobre cómo gestionarlos.

8. La Directiva europea de protección del informante (*whistleblowing*), incluye expresamente a los incidentes de seguridad dentro de su alcance[16]. Dicha norma ha sido transpuesta al ordenamiento jurídico español a través de la Ley 2/2023, de 20 de febrero.

[16] DIRECTIVA (UE) 2019/1937 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.
https://www.boe.es/doue/2019/305/L00017-00056.pdf