Bruselas convierte la ciberseguridad en estratégica con la aprobación de la directiva NIS2 y el reglamento DORA

El 27 de diciembre se publicaba en el Diario Oficial de la Unión Europea, la Directiva UE 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS 2) y el Reglamento UE 2022/2554 de Resilienci

Más obligaciones para las empresas en materia de ciberseguridad, en un contexto ya exigente y en el que recientemente se ha sabido que el Banco Central Europeo (BCE) ha anunciado que multará a Abanca con 3,145 millones de euros por no informar a las autoridades que había sido víctima de un ciberataque en el plazo máximo que establece el organismo.

El caso se remonta a 2019, cuando el banco sufrió un ataque a sus sistemas informáticos, que fueron infectados por un malware. En ese momento, **Abanca respondió suspendiendo todos sus servicios bancarios de web y móvil**, así como sus cajeros automáticos y sus servicios de pago SWIFT. Ahora podría recurrir al TJUE ese fallo judicial.

Mientras que DORA quiere crear un marco armonizado a nivel europeo en cuanto al desarrollo digital del sector financiero que mitigue las ciberamenazas de entidades financieras de toda índole, incluidas proveedores de criptoactivos, NIS 2, reemplazará a NIS 1 para dotar mas robustas medidas de ciberseguridad en los sectores críticos tanto del sector público y privado. **DORA se aplicará en enero del 2025 y NIS 2 debe trasponerse antes de octubre del 2024.**

Una puesta incondicional por ciberseguridad

Carlos Sáiz, vicepresidente de ISMS Forum y presidente de la asociación de abogados expertos en tecnología ENATIC, sostiene que “vivimos un momento similar al que se vivió en protección de datos hace cinco o seis años donde la aprobación del RGPD europeo ha sido clave para luego cambiar nuestra ley de privacidad. En este caso la aprobación de la Estrategia Nacional de Ciberseguridad, pese a no haber régimen sancionador, ha sido clave para las empresas públicas. En el caso de las empresas, ante cualquier norma, siempre han mejorado sus prestaciones”.

Otra cuestión que destaca Sáiz es que “se acabó la voluntariedad, porque este tipo de normativa obliga a las empresas a ser responsables y a tomar medidas de protección de sus activos. La llegada de DORA va a reforzar las políticas de seguridad en el sector financiero, ya acostumbrado a contar con una regulación notable».

Desde su punto de vista, “al final lo que se respalda es la gobernanza de las empresas, con nuevas obligaciones para los Consejos de Administración que serán responsables últimos y más importancia al CISO, director de seguridad de las empresas cuya visión no es solo técnica sino también estratégica en estos momentos para las empresas. **Ahora la ciberseguridad es clave cuando una empresa se plantea lanzar un nuevo producto o servicio”.**

Sobre la sanción del BCE a Abanca, por notificar un incidente de seguridad fuera de plazo: “Las empresas deben seguir a rajatabla el protocolo existente. La empresa gestionó bien el incidente y tuvo poco impacto, pero **el peso de la sanción viene por esa notificación a la autoridad de control fuera de dicho plaz**o. Es importante contar con responsables de ciberseguridad que puedan hacer su trabajo y tengan os medios adecuados”.

Sáiz destaca dos cuestiones claves a corto y medio plazo: “**La necesidad de controlar la cadena de suministro de las empresas y que los proveedores cuenten con una política de ciberseguridad adecuada**. Las normas obligan a grandes compañías, pero detrás de ellos hay muchas empresas que constituyen su cadena de suministro. Tendrán que adoptar esos parámetros, sin duda”.

Al mismo tiempo, revela otro tema importante: **“Es sustancial ampliar los aspectos de compliance al mundo de la ciberseguridad**. Estas áreas necesitan definir los mapas de riesgos que se derivan de esta normativa que entra en vigor en los próximos meses. Hay compañías que están afectadas por estas normas Son tantas obligaciones que es necesario definir un mapa de riesgo normativo sobre que obligaciones deben cumplir y definir un sistema de compliance adecuado”.

Gestionar el riesgo tecnológico

Por su parte, **María Vidal**, socia responsable de práctica de protección de datos y nuevas tecnologías de la boutique especializada finReg, advierte que “el caso del **reglamento DORA crea un código normativo sobre gestión del riesgo tecnológico para las entidades financieras y para los proveedores tecnológicos** que prestan servicios a esas entidades”.

“Esta compilación normativa faculta a las autoridades financieras para supervisar la implantación de estas medidas, por lo que **estas autoridades tendrán que estar preparadas y contar con las aptitudes para esos trabajos de control** en materia de gestión de riesgo tecnológico, a partir de enero del 2025”, indica.

En los próximos años, veremos perfiles muy tecnológicos sentados en los consejos de administración

Respecto a la directiva NIS2, **esta directiva se centra “en la creación de una estrategia común de ciberseguridad de todos los Estados miembros**, en la compartición de información sobre incidentes de ciberseguridad y en la designación tanto de autoridades competentes responsables de la gestión de incidentes y de las crisis de ciberseguridad a gran escala, que forman un Grupo de Cooperación entre estos Estados”.

Junto a ello también se ocupa de “**equipos de respuesta a incidentes de seguridad,** conocidos por CSIRT, por las siglas inglesas de computer security incident response team, y una red nacional de estos equipos, asi como una red europea de organizaciones de enlace para las crisis de ciberseguridad a fin de gestionar coordinadamente los incidentes y las crisis a gran escala entre los Estados miembros (formada por representantes de las respectivas autoridades de gestión de crisis de ciberseguridad).

A su juicio, para cumplir estas nuevas normativas, las entidades tendrán que trabajar en frentes como el de contar “con un marco de gestión del riesgo que incorpore una nueva línea de defensa para el **control, gestión y supervisión de los riesgos tecnológicos** que asegure una capacidad de recuperación adecuada y para el seguimiento de los acuerdos con los proveedores de servicios tecnológicos”.

Ora cuestión importante será “la **introducción de muchos cambios en la gobernanza**. En los próximos años, veremos perfiles muy tecnológicos sentados en los consejos de administración, dado el nivel de conocimientos requerido para la toma de decisiones sobre estas normas”.

También cree que será necesario “**implantar de un marco de control en toda la cadena de suministro**, que supondrá un inventario actualizado de proveedores, la identificación de todos los subcontratistas intervinientes, de las transferencias internacionales de datos aparejadas y un detalle mucho más exigente en los niveles de calidad de los servicios con estos terceros”.

Por último, Vidal considera que “**habrá la exigencia de evidencias reales de evaluación de las vulnerabilidades de las compañías**, como la realización de pruebas de penetración basadas en amenazas internas y a proveedores. La norma no quiere promesas que se queden en el papel de un contrato, exige evidencias de que se realizan los controles concretos”.

Replantear la ciberseguridad como riesgo legal y de negocio

Por su parte, **Francisco Pérez Bes**, socio del área digital de Ecix y ex secretario general de INCIBE: “Este concepto de la ciberseguridad la que debe guiar a las empresas afectadas por esta nueva regulación, que deben evolucionar de la concepción de la protección de la organización (evitar sufrir un ciberataque) al de la resiliencia, entendida como la capacidad para reponerse a un incidente de ciberseguridad”.

A su juicio, “**es aquí donde cobra importancia el diseño de una gobernanza sólida**, que incluya procesos que permitan acreditar el cumplimiento de las obligaciones que impone la nueva normativa, puesto que la ciberseguridad ha dejado de ser una obligación de fines para convertirse, de una vez por todas, en una obligación de medios basada en una gestión del riesgo”.

Desde esta perspectiva, “**las empresas deberán mantener sus esquemas de seguridad técnicos**, con medidas técnicas eficaces y adecuadas en función de los riesgos a los que se enfrenta la empresa (esto es, las ciberamenazas, siempre cambiantes y cada vez más sofisticadas); pero, sobre todo, las medidas organizativas».

“Y esto último se pretende lograr exigiendo a los órganos de dirección de las empresas (y sus empleados) a que estén formados en ciberseguridad, e **imputándoles responsabilidad legal por su actuación poco diligente a la hora de tomar decisiones** sobre cómo proteger a sus organizaciones”, destaca.

En este sentido, este experto coincide con la valoración de que la nueva ciberseguridad encaja bien en el sistema de cumplimiento normativo de las empresas, con tal de poder modular su propia responsabilidad. Pero también -añade- para mejorar la resiliencia de las empresas con el objetivo de reforzar su competitividad en el mercado y mejorar la confianza de los inversores.

“No olvidemos que el sector de los ciberseguros ya ha avisado de la imposibilidad de asegurar todos los ciberriesgos de las empresas, por lo que las compañías van a tener que hacer grandes esfuerzos con tal de mitigar esos riesgos que probablemente no obtengan cobertura aseguradora y deban asumir ellas mismas”, recuerda.

Para este jurista, autor del Código electrónico de Derecho de la Ciberseguridad publicado por el Boletín Oficial del Estado y Director del memento experto de ciberseguridad, «esta normativa también deja entrever una serie de medidas coercitivas de buen seguro controvertidas».

“Así, por ejemplo, **destaca la posibilidad de apartar temporalmente al Director General de aquellas empresas que decidan no aplicar las recomendaciones de ciberseguridad emitidas desde la autoridad competente;** o el proceso para imponer sanciones, que va a requerir dotar de competencias inspectoras y sancionadoras claras a los organismos competentes; o, por citar alguna otra, los breves plazos de notificación de incidentes, o la posibilidad de requerir antecedentes penales de determinados trabajadores de entidades designadas críticas, lo que plantea cuestiones relevantes desde la óptica de la protección de datos”, nos recuerda.

Una normativa clave para las empresas

Vicente Moret, letrado en Cortes Generales y «Of counsel» de Andersen en España, experto en el mundo de la ciberseguridad, advierte que hay una triple normativa que pretende modificar de forma notable el marco actual en la UE: “Bruselas se comprometió a aprobar este paquete normativo antes del 2023 que está interconectado entre sí”.

A ese respecto recuerda que “la directiva de Resiliencia de entidades críticas es más general, que sustituye a la del 2018 coordinándola con otras nomas. De ahí pasamos a NIS2 y a DORA que es un reglamento centrado en las entidades financieras. **Marcará, sin lugar a dudas, un antes y un después en Europa en materia de ciberseguridad.** Habrá que ver como se traspone NIS2 en España por la importancia que tiene en el plazo de dos años”.

En el caso de NIS2, “**plantea obligaciones para empresas y sectores estratégicos en dos niveles,** primero por sectores tradicionales como banca, telecomunicaciones, agua, energía, transporte, alimentación, farma o logística por citar algunos y luego por volumen. Todo lo que no sea pyme, hasta 250 trabajadores y 50 millones de facturación acaba en esta directiva”.

Para este jurista, “**el colmo de la sofisticación es el reglamento DORA**. Es un Reglamento europeo lo que implica su aplicación directa, pese a ello se ha establecido un periodo transitorio de unos veinticuatro meses”. A su juicio es obvio que las empresas tendrán que desarrollar sus políticas específicas de compliance en materia de ciberseguridad”.

“**Es la primera vez que se utiliza una normativa de este tipo para canalizar la necesidad de regular la seguridad digital en el sector financiero.** No es solo banco, su aplicación será para aseguradoras, agencias de valores o infraestructuras de mercados financieros, así como proveedores de servicios digitales e incluso las empresas de criptomonedas están incluidas ahí. Todo lo que maneje dinero en la UE y no sea pyme está incluido en DORA”.

A su juicio, **es evidente que esta nueva normativa que se transpondrá en nuestro país va a ser muy exigente tanto para las empresas públicas como privadas**: “El futuro es digital y parte de su cumplimiento supone contar con la seguridad adecuada en este tipo de negocios. Supone un cambio en la gobernanza de las compañías importante con obligaciones para el Consejo de Administración y el propio CISO con un estatuto definido de obligaciones y derechos”.

Fuente: economistjurist.es

Link: https://www.economistjurist.es/zbloque-1/bruselas-convierte-la-ciberseguridad-en-estrategica-con-la-aprobacion-de-la-directiva-nis2-y-el-reglamento-dora/