La Directiva NIS, un paso necesario al que le falta mucho recorrido

A mediados del año pasado la Unión Europea aprobó la Directiva (UE) 2016/1148, conocida como Directiva NIS, la cual aborda la seguridad de redes y sistemas de información con el objetivo de mejorar la respuesta de las empresas e instituciones ante los incidentes. Ahora, esta normativa debe ser adaptada por los Estados miembros a sus respectivos ordenamientos jurídicos antes del 9 de mayo de 2018. Sin embargo, esto plantea una serie de interrogantes, algunos de los cuales se intentaron responder en esta mesa.

De izda. a dcha. en primera fila: Ana Borredá, de RED SEGURIDAD y Fundación Borredá; Javier Zubieta, de GMV; Enrique Polanco, de Global Technology 4E; José Valiente; del Centro de Ciberseguridad Industrial; y Yolanda Duro, de RED SEGURIDAD. En segunda fila, de izda. a dcha.: Pablo Municio, de Deloitte; Xavier Mitxelena, de S21sec; Rafael Santos, de ISMS Forum; Javier García Carmona, de Daranorte; y David Marchal, de RED SEGURIDAD. Al fondo, de izda. a dcha: Enrique González, de RED SEGURIDAD; y Antonio Martínez, de Metro de Madrid.

Tx: David Marchal
Ft: RED SEGURIDAD

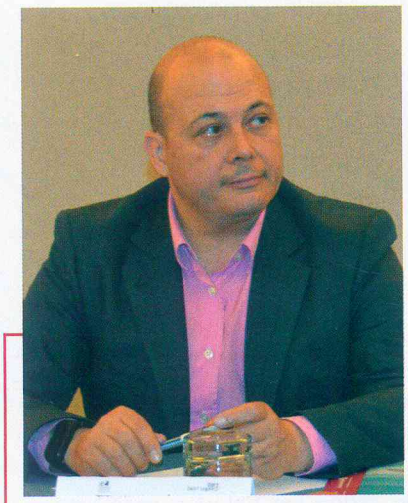
El pasado 19 de julio, el Diario Oficial de la Unión Europea publicó el texto de la Directiva 2016/1148, conocida comúnmente como Directiva NIS; un documento cuya finalidad es establecer unas medidas que garanticen la seguridad de las redes y sistemas de la información en todos los países de la Unión. De esta manera, se crean, por tanto, unos mínimos comunes de protección con la intención de romper con las diferencias actuales entre los Estados en cuanto a la ciberseguridad se refiere. Además, como señaló en su momento el europarlamentario Andreas Schwab, "incrementará la colaboración y el intercambio de información para hacer frente a las crecientes amenazas tecnológicas, especialmente aquéllas que puedan afectar a varios países simultáneamente".

Por tanto, la importancia de esta normativa es enorme, y más si tenemos en cuenta que España deberá incorporarla ahora a su ordenamiento jurídico. Precisamente, para conocer mejor lo que representa esta legislación y de qué forma se puede producir esa adaptación, la revista RED SEGURIDAD, con el patrocinio de la **Fundación Borredá**, organizó una mesa redonda para debatir sobre este tema con distintos expertos del sector.

Lo primero que quedó claro, y fue opinión compartida por todos, es la necesidad que existía de tener una norma europea de estas características. Por ejemplo, para **José Valiente**, director del Centro de Ciberseguridad Industrial (CCI), "resulta muy positiva, porque va a impulsar mucho la cultura de seguridad en las organizaciones". De igual forma opinó **Javier García Carmona**, responsable de la consultora Daranorte, para quien la Directiva supone "un paso cualitativo y cuantitativo importante", puesto que "se partía de cero". **Rafael Santos**, representante de ISMS Forum, indicó que se trata de "un marco de referencia" que establece "los requisitos mínimos para que lo puedan cumplir todos los Estados miembros", comentó durante su intervención.

En general, todos los expertos coincidieron en la idea que resumió **Xavier Mitxelena**, vicepresidente del Consejo de Administración de S21sec: "Es un primer estadío, una directiva de mínimos para entender la sensibilidad del legislador", explicó.

Ahora bien, más allá de eso, la normativa ha dejado un sabor de boca agridulce entre los presentes en la mesa redonda. Para **Pablo Municio**, gerente de riesgos IT de Deloitte, "si bien es un buen esfuerzo, es necesario continuar avanzando y concretando aspectos como los requerimientos que afectarán a los operadores de servicios y proveedores TIC. Actualmente se centra más en el modelo de actores y en la construcción de la red de CSIRT [Equipos de Respuesta a Incidentes de Seguridad Informática, por sus siglas en inglés]". Se trata de una afirmación que también comparte García Carmona, de Daranorte: "En este nuevo escenario de regulación se han preocupado en un 80 por ciento más de la parte estructural, con la creación de los distintos mecanismos de ciberseguridad, y han dejado sólo un 20 por ciento para la base, con la definición de operadores, medidas apropiadas en aspectos de seguridad, notificación incidentes, etcétera". De hecho, este profesional echa en falta "un poco más de equilibrio" en este sentido.



José Valiente

Director del Centro de Ciberseguridad Industrial

"La Directiva NIS y la Ley PIC tienen grandes diferencias por los sectores afectados. Hay que tenerlo en cuenta porque la primera afecta a una parte mínima comparada con la segunda"

Precisamente, el punto de vista del operador estuvo representado a través de **Antonio Martínez**, responsable de Seguridad Informática de Metro de Madrid. Para Martínez, esta legislación también deja aspectos sin definir desde el punto de vista de los operadores. "Es un tanto ambigua y nos va a suponer muchos esfuerzos para ver cómo pueden converger todas las leyes que hay sobre la mesa", indicó.

De igual forma se pronunció **Javier Zubieta**, responsable de Desarrollo de Negocio de Ciberseguridad de GMV: "Por un lado, estamos avanzando y haciendo esfuerzos para cumplir la Ley PIC [Ley sobre Protección de las Infraestructuras Críticas]. Ahora hay que adaptar también la Directiva NIS, que se juntará en 2018 con la obligatoriedad para las empresas de cumplir el Reglamento General de Protección de Datos de la UE. Por tanto, los operadores privados se tendrán que poner las pilas para adaptarse a las tres", explicó.

No en vano, las infraestructuras críticas son el ámbito en el que la Directiva NIS afectará más de lleno, tal y como recordó **Enrique Polanco**, socio director de Global Technology 4E. "Parece que el objetivo de esta legislación es crear normativa para que las compañías de estos sectores reporten sus incidentes. Habrá que ver cómo se transpone al ordenamiento jurídico español", observó. Porque, a juicio de Polanco, hay diferencias entre la Ley PIC y la Directiva NIS en determinados conceptos y en los sectores que se pueden ver afectados.

La transposición de la Directiva

A partir de ahí, el debate se focalizó en saber de qué manera puede llevar a cabo esa transposición la Administración española. Martínez, de Metro de Madrid, cree necesaria la existencia de "una autoridad o punto único común" que sirva de elemento de coordinación. "Crear nuevas estructuras implica destinar recursos y desaprovechar años de conocimiento;

Javier García Carmona

Responsable de Daranorte

"Para la transposición de la Directiva NIS, es necesario que haya una estructura clara y definitiva del estamento o estamentos que desempeñarán las funciones de órgano de coordinación"

además, hay organismos sectoriales que requieren también comunicaciones de incidentes. Si tenemos que reportar a cada uno de ellos de forma distinta, puede suponer un problema", explicó.

Por eso, abogó por la creación de "una ventanilla única", porque resulta "más lógico optar por algo normalizado y estándar, y también es una forma de optimizar recursos". Claro que, puntualizó el invitado, "otra cosa es que haya decisiones políticas detrás para aprobar la creación de un organismo desde cero".

Al respecto también se pronunció Santos, de ISMS Forum, quien puso sobre la mesa el caso de las empresas públicas que están integradas en el Estado. Ellas tienen la obligación de gestionar los incidentes según el Esquema Nacional de Seguridad y reportarlos al CERT del Centro Criptológico Nacional (CCN-CERT), pero si se trata de una infraestructura crítica, tienen que hacer-

Rafael Santos

Representante de ISMS Forum

"Dado que se está elaborando la transposición de la Directiva NIS, el sector debe aprovechar la situación para decir lo que considere que puede aportar"

lo al CERT de Seguridad e Industria (CERTSI). "Para ellos es un problema. ¿Cómo diferencian los incidentes relacionados con las infraestructuras críticas de los de la propia organización? Y ahora la Directiva NIS recoge que tiene que haber una única autoridad. ¿Cuál será?", reflexionó Santos.

Por todo ello, este CISO apuntó la importancia de que las administraciones competentes "lo dejen claro desde el principio, porque eso puede dar lugar a nuevos problemas *a posteriori*". "Ahora, que se está trabajando en hacer la transposición de la Directiva, es el momento de hacerlo", recalcó.

García Carmona, de Daranorte, también es consciente de la situación compleja que se genera. "El Estado tendrá que establecer un criterio único y fijar cómo será. Es necesario que haya una estructura clara y definitiva con nombre y apellidos de los estamentos que desempeñarán las funciones de órgano de coordinación".

Sin duda, éste fue uno de los temas que más preocupó a los asistentes a la mesa redonda, puesto que, además, afecta a una gran cantidad de sectores económicos involucrados. Valiente, del CCI, sacó a colación un informe realizado en Reino Unido en 2013, "cuando se comenzaba a hablar de la necesidad de legislar la seguridad de las redes y los sistemas de la información en los países de la Unión Europea". Según el invitado, se llegó a la conclusión de que el impacto de la Directiva NIS cuando se aprobara afectaría a 23.000 empresas de ese país; y el sector más afectado de todos, con el 73 por ciento, sería el de la salud, seguido por el de transporte y el financiero.

Al respecto, Polanco, de Global Technology 4E, señaló que "hay que aprovechar la importancia que la Directiva NIS le da al sector de la Salud, como uno de los más afectados, para integrar todos estos conceptos de ciberseguridad en el Plan Estratégico Sectorial de Salud que actualmente elabora el CNPIC".

El modelo PIC

A continuación, los invitados hicieron hincapié en las conexiones entre la Directiva NIS y la Ley PIC, a pesar de que existen diferencias como que la primera establece siete sectores de actuación y la segunda abarca hasta 12. "La Ley PIC y la Directiva NIS tienen grandes diferencias por los sectores afectados. Esto hay que tenerlo en cuenta, porque la primera afecta a una

Xavier Mitxelena

Vicepresidente del Consejo de Administración de S21sec

"Lo importante es que todas las empresas del sector ayudemos, porque si no somos capaces de colaborar, estamos perdidos. Los problemas que se pueden dar en ciberseguridad son muy serios"

Resumen de la Directiva NIS

1.- Establece obligaciones para que todos los Estados miembros adopten una estrategia nacional sobre la seguridad de los sistemas de redes y la información.

2.- Crea un Grupo de Cooperación con el fin de apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y para desarrollar la confianza entre ellos.

3.- Impulsa una red de equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés), con el fin de contribuir a mayor confianza entre los Estados miembros y promover la cooperación operativa rápida y eficaz.

4.- Establece los requisitos de seguridad y notificación de los operadores de servicios esenciales y para los proveedores de servicios digitales.

5.- Determina las obligaciones para que los Estados miembros designen las autoridades competentes en el ámbito nacional, puntos de contacto únicos y CSIRT, con tareas relacionadas con la seguridad de redes y sistemas de información.

parte mínima en comparación con la segunda", aseguró Valiente, de CCI.

Eso sí, en lo que todos los presentes estuvieron de acuerdo es en que la implantación en España del modelo de protección de infraestructuras críticas puede aportar muchas lecciones aprendidas a la hora de adaptar la nueva normativa europea. Y partiendo de la base de que la Administración española cuenta con una serie de limitaciones en cuanto a la disposición de recursos o la contratación de personal, la necesidad de integración todavía resulta más importante.

En palabras de Santos, de ISMS Forum, "hay que unificar los recursos disponibles, porque si no es así, no vamos a ser capaces de poder cumplir ninguna norma", sentenció. El directivo, de hecho, cree fundamental poner para este fin a un grupo de personas que se encargue de ello.

No obstante, hay quien no lo ve tan claro. Por ejemplo, García Carmona, de Daranorte, puso sobre la mesa el problema del "protagonismo administrativo", en tanto en cuanto hay muchas instituciones afectadas y todas quieren tener su protagonismo. Por eso, para el directivo, lo mejor es que el propio Gobierno tome las riendas y desarrolle "una ley que recoja todas las singularidades que haya", matizó.

En este sentido, para Municio, de Deloitte, es importante que se concreten ciertos aspectos como los umbrales de incidentes, los formatos de reporte o las herramientas empleadas para ello. Además, "los impactos asociados a incidentes de seguridad varían en función de cada sector; a modo de ejemplo, no tendría el mismo impacto para la sociedad el fallo de una infraestructura energética o de un nodo de comunicación que otras infraestructuras con menor grado de cobertura, por lo que, del mismo modo, las exigencias a nivel de *reporting* y comunicación de brechas de seguridad, deberían estar alineadas con estos factores", opinó. Asimismo, apuntó: "además, las estructuras y recursos también varían de un sector a otro, va a ser difícil pedir a un hospital que reporte las brechas de seguridad a diferentes reguladores y en diferentes formatos; se requiere estructura y capacidades para ello".

Los asistentes a la mesa coincidieron en señalar la importancia de establecer sanciones a las empresas que se salten los preceptos de la Directiva NIS.

Con esta afirmación se mostró de acuerdo Mitxelena, de S21sec, para quien es importante que la Administración "legisle con lógica" y detalle cuestiones como "de qué forma se han de medir los incidentes, cuáles serán los baremos para establecer los distintos tipos de incidentes, etcétera". Y es que, si no se hace así, para el directivo, "al final ocurrirá algo pronto que hará correr a todo el sector".

Colaboración público-privada

A partir de aquí se abordó el tema de la importancia de la colaboración de las administraciones con la industria privada a la hora de implantar la Directiva NIS. Para Martínez, de Metro de Madrid, "la coordinación depende de la voluntad; es decir, de que se quiera colaborar". Claro que, para este profesional, sólo se puede conseguir avanzando en la misma dirección,

La importancia de los CSIRT en la Directiva NIS

Una de las grandes novedades de la Directiva NIS es la creación de una red de equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés), que estará compuesta por el conjunto los CSIRT nacionales que tendrán que designar cada uno de los países de la Unión Europea.

Según esta normativa, esta red se crea para "contribuir al desarrollo de la confianza y seguridad entre los Estados miembros, así como para promover una cooperación operativa rápida y eficaz". Así pues, cada país deberá adoptar una serie de medidas y decisiones conforme a sus necesidades para adaptarse a esta Directiva.

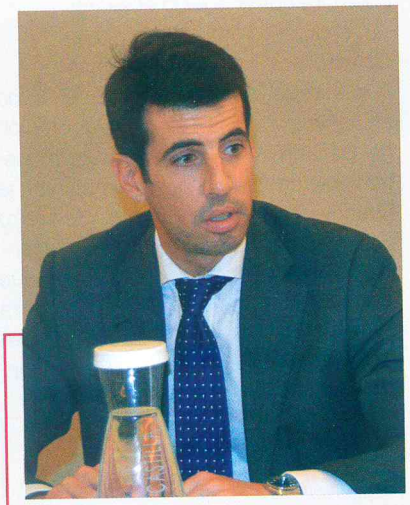
De hecho, la norma les hace responsables de garantizar unos niveles de seguridad tecnológica óptimos en dos tipos de organizaciones. Por un lado, los operadores de servicios esenciales de los siete sectores empresariales que delimita la norma como ámbito de actuación: Energía, Transporte, Banca, Mercados financieros, Sanitario, Suministro y distribución de agua potable e Infraestructuras digitales. Por otro, a los proveedores de servicios digitales, como pueden ser los motores de búsqueda o los servicios *cloud*. No obstante, la Directiva no se aplicará a las microempresas y pequeñas empresas dedicadas a estas actividades.

aportando todos los actores involucrados, sin esconder información, no poniendo trabas... "Solo cuando esto se dé, se podrán dar pasos en la línea de la colaboración", apuntó.

Mitxelena, de S21sec, recalcó también la importancia de la "transparencia" en este proceso. "Lo importante es que todos ayudemos, porque si no somos capaces de colaborar, estamos perdidos. Los problemas que se pueden dar en ciberseguridad son muy serios. Por eso, las propias situaciones que se vayan sucediendo son las que nos van a obligar a estar coordinados".

Por su parte, Zubieta, de GMV, fue un paso más allá al apuntar la necesidad de exigir a los CSIRT que colaboren entre ellos. "Si uno está obligado a reportar incidentes a este tipo de organismos, pero luego no se coordinan entre ellos, no se podrán beneficiar de las buenas prácticas y de la experiencia que hayan tenido otras empresas", comentó, para después añadir que, de esa forma, "sí se puede llegar a conseguir una colaboración efectiva".

De igual forma se manifestaron el resto de los asistentes. Por ejemplo, Santos, de ISMS Forum, defendió el actual modelo de colaboración entre los CERT nacionales y la confianza que hay para comunicarse entre ellos. "Tenemos que aprovechar ese modelo, porque si esto se traslada, puede ser posible la colaboración", apuntó. Se trata, como se encargó de resaltar García Carmona, de Daranorte, de "crear algo, pero sin romper con lo que ya hay". A su juicio, "hace falta una capa de coordinación y de gobierno para poder hilvanar todas las partes".



Pablo Municio

Gerente de riesgos IT de Deloitte

"Los impactos asociados a incidentes varían en función de cada sector; las exigencias a nivel de 'reporting' y comunicación de brechas de seguridad, deberían estar alineadas con esos factores específicos"

El papel de los operadores

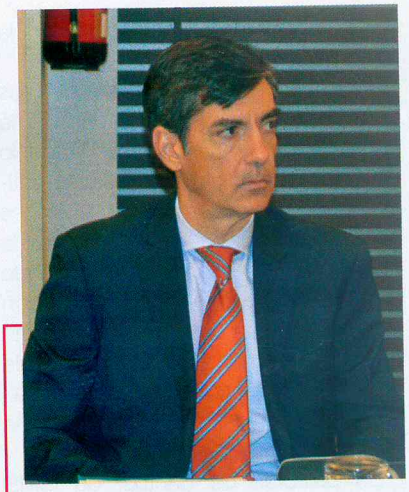
Una vez analizadas las implicaciones que debe tener la adaptación de la Directiva al ordenamiento jurídico español, los asistentes centraron su atención en los operadores de servicios esenciales y los proveedores de servicios digitales, puesto que tanto unos como otros tendrán la obligación de establecer medidas mínimas de seguridad para proteger sus redes y sistemas de la información.

Sin embargo, la definición de los segundos no deja de estar muy clara. Así lo expresó Mitxelena, de S21sec, para quien, según su interpretación, "los proveedores de servicios digitales se pueden referir a empresas que dan soporte a los distintos sectores afectados". En palabras de Antonio Martínez, "parecen empresas que dan servicio a operadores, más que operadores en sí mismos".

En cualquier caso, la norma indica que estas compañías tendrán que trasladar sin dilación a la autoridad competente o al CSIRT nacional aquellos incidentes de seguridad que sufran y puedan afectar a la continuidad de sus actividades. Claro que, en caso de no cumplirse, la Directiva obliga a los Estados miembros a que establezcan un régimen de multas "efectivas, proporcionadas y disuasorias" para las empresas que no sigan sus disposiciones.

A juicio de todos los expertos asistentes, las sanciones son necesarias para que todas las organizaciones acaben cumpliendo la norma. Y es que, como señaló García Carmona, de Daranorte, "mientras que no haya sanciones, no se hace nada".

Por su parte, Mitxelena, de S21sec, apuntó en el mismo sentido. Ahora bien, el directivo matizó que también depende de la cuantía de las multas, ya que algunas empresas pueden verse tentadas a saltarse las normas porque obtienen muchos beneficios que les permiten hacerlo. Por eso, según Mitxelena, es preciso también "cambiar las actitudes" de los directivos. Algo que ya se está produciendo, tal y como apuntó Martínez, de Metro de Madrid, con la reciente reforma del Código Penal, que ha impulsado "la concienciación por parte de los responsables de las organizaciones".



Antonio Martínez

Responsable de Seguridad Informática de Metro de Madrid

"La Directiva NIS es un tanto ambigua sobre los operadores, por lo que nos va a suponer muchos esfuerzos para hacer que converjan todas las leyes que hay en el ordenamiento jurídico español"

En otras palabras, como afirmó García Carmona, de Daranorte, se trata de fomentar "la conciencia al respecto y la formación, porque España es un país acostumbrado a las sanciones".

Y en este contexto, la homologación también ayudará a remover muchas conciencias. "Es importante apostar por los conceptos de calidad y compromiso, y también exigirlos", puntualizó Mitxelena, de S21sec. Y es que, para el

Javier Zubieta
Responsable de Desarrollo de Negocio de Ciberseguridad de GMV

"Los operadores privados tendrán que ponerse las pilas para adaptarse a tres normas: la Ley PIC en la que ya estamos haciendo esfuerzos, la Directiva NIS y el RGPD, que se aplicarán a partir de 2018"

directivo, comprar servicios baratos sin ningún tipo de homologación genera problemas, "porque lo que se adquiere es la continuidad de un negocio que afecta a la sociedad", matizó.

Al respecto, Polanco, de Global Technology 4E, apuntó que ya se está avanzando en este sentido, pues "a las empresas de seguridad se les exige que, al menos, cuente con alguna certificación de seguridad como puede ser la ISO27001, y como tal ya aparece en muchas licitaciones del Estado", comentó. Por su parte, a juicio de Zubieta, de GMV, "estos requisitos ya se han asumido como algo normal y una obligación del mercado en cualquier proceso de licitación para las empresas del sector".

Conclusiones

Para terminar, los asistentes hicieron un breve resumen de lo que supone la Directiva NIS para nuestro país. A juicio de Mitxelena, de S21sec, se trata de "una gran oportunidad para España, porque nos encontramos en ventaja con respecto a Europa", pues ya tenemos una legislación que aborda muchos aspectos de los que se trata en la normativa europea. Eso sí, según el directivo, hay que ser "abiertos de mente", "tener generosidad" y llevar a cabo "un modelo transversal para la transposición". En este sentido, confirmó, la Ley PIC ha sido "un gran acierto", con la que se ha ido a "un buen ritmo", y ha supuesto "una oportunidad tanto para el sector como para la Administración", recalcó.

En esa línea, Polanco, de Global Technology 4E, también comparó la nueva Directiva NIS con la Ley PIC y, al igual que esta última, expresó su deseo de que la primera vaya "de arriba a abajo", con el fin de que una instancia superior "desarrolle y unifique desde ahí todos los criterios sobre ciberseguridad".

Por su parte, Zubieta, de GMV, demandó a los entes públicos que se hagan cargo de su redacción que "velen por que se desarrolle bien", y que "se tengan en cuenta el resto de leyes que pueden verse afectadas". Para ello, según apuntó Municio, de Deloitte, y Valiente, del CCI, "es buena oportunidad para aprovechar lo hecho". Y no sólo eso. "Puesto que nos encontramos en un momento en el que se está elaborando la transposición de la Directiva, hay que beneficiarse de ello para que el sector pueda decir lo que considera que se puede aportar", afirmó Santos, de ISMS Forum.

Enrique Polanco
Socio director de Global Technology 4E

"Hay que aprovechar la importancia que la Directiva NIS le da al sector de la Salud como uno de los más afectados, para integrar todos esos conceptos de ciberseguridad del PES de Salud que está elaborando el CNPIC"

En definitiva, tal y como cerró la mesa redonda García Carmona, de Daranorte, "nos encontramos ante un gran cambio que se empieza con pequeños pasos". ■

Uno de los principales temas de debate fue establecer de qué forma las autoridades españolas competentes podrán adaptar la Directiva NIS a la legislación del país.