ENCUENTRO EXPANSIÓN - CIPHER (PROSEGUR)

Qué exige a las empresas la nueva directiva europea de ciberseguridad

RIESGOS/ Las compañías se preparan para hacer frente a los requisitos de NIS2, una normativa que impondrá sanciones duras a quienes no extremen precauciones contra los ciberdelincuentes.

Jesús de las Casas. Madrid

En respuesta al incremento exponencial de los ciberataques en los últimos años, el Consejo de Europa y el Parlamento Europeo llegaron a un acuerdo para lanzar una nueva directiva de seguridad de información de redes. Se trata de NIS2, que entró en vigor el 27 de diciembre de 2022. Desde entonces, los Estados miembros de la UE cuentan con un periodo máximo de 21 meses para transponer la directiva a sus respectivos ordenamientos jurídicos.

Los requisitos que esta regulación exigirá a las empresas se trataron en el encuentro *El impacto de la normativa NIS2 en los directivos y consejeros*, que organizó EXPANSIÓN con el patrocinio de Cipher, la compañía especializada en ciberseguridad de Prosegur.

Jose Luis Pindado

Iñaki Garay, director adjunto de EXPANSIÓN; David Fernández Granado, director general de Cipher; Margarita Fernández de Prada, directora de transformación digital de Iberdrola; Carlos Rodríguez Sanz, responsable regional del negocio 'cyber' para Europa y Asia-Pacífico de AXA XL; José Seara, fundador y consejero delegado de DeNexus; y Carlos Pelegrín Fernandez, socio de Corporate Learning Solutions de Esade.

Asignaturas pendientes

La llegada de la nueva directiva plantea algunos retos clave para las compañías. David Fernández Granado, director general de Cipher, destacó los más importantes: "Deben contar con visibilidad total sobre el perímetro de seguridad, evitar la fragmentación tecnológica y organizativa, profesionalizar la función incorporando talento de ciberseguridad e implementar mecanismos de mejora continua para adaptarse a la velocidad de los cambios". Pese a que aún queda camino por recorrer, Fernández Granado subrayó que "España está progresando de forma adecuada con el liderazgo de las grandes empresas, y tenemos una gran oportunidad para posicionarnos como referente en ciberseguridad".

Dado que NIS2 extenderá la responsabilidad personal a los consejeros y directivos, se prevé un aumento en la demanda de ciberseguros, sobre todo en el segmento de *middle market*. Así lo consideró Carlos Rodríguez Sanz, responsable regional del negocio *cyber* para Europa y Asia-Pacífico de AXA XL, que apuntó que "el ciberseguro es la póliza de incendios del siglo XXI: la ciberseguridad debe ser una inversión proactiva para adelantarse a los ataques y amenazas". Tras una década de experiencia en el mercado español, Rodríguez Sanz recalcó que "la forma de evaluar el riesgo ha cambiado: ahora se diseña según el perfil de cada empresa".

Asimismo, "una de las novedades de NIS2 es el fomento de la colaboración público privada para favorecer la integración de nuevas tecnologías y el desarrollo de proyectos que contribuyan a mitigar estos riesgos", apuntó José Seara, fundador y consejero delegado de DeNexus. Para la compañía, que se centra en la cuantificación financiera de este riesgo, "trasladar la importancia de la ciberseguridad a los directivos requiere hablar su idioma de negocio, en lugar de anclarse en la parte técnica".

Carlos Pelegrín Fernandez, socio de Corporate Learning Solutions de Esade, confirmó que "la nueva directiva cambia mucho las cosas para los directivos y consejos de administración: el interés en la ciberseguridad crecerá de un modo muy importante". Esta tendencia ya viene quedando de manifiesto en los últimos años con la incorporación de perfiles tecnológicos a los consejos. "Cuanto más independientes y mejor formados estén los consejeros que van entrando, mejor", resaltó Pelegrín.

Desde la perspectiva de las compañías, "la digitalización es una ventaja pero, al mismo tiempo, es un aspecto que nos hace más vulnerables ante potenciales ciberataques", reconoció Margarita Fernández de Prada, directora de transformación digital de Iberdrola. La nueva directiva viene a reivindicar la necesidad de destinar más recursos a la ciberseguridad. Así, "NIS2 no es algo disruptivo para nosotros porque ya teníamos estas obligaciones, pero sí supone una oportunidad para poner estos temas sobre la mesa de los consejos", concluyó Fernández de Prada.

CARLOS RODRÍGUEZ
Responsable regional del negocio 'cyber' de AXA XL

"La ciberseguridad debe ser una inversión proactiva para adelantarse a los ataques y amenazas"

DAVID FDEZ. GRANADO
Director general de Cipher

"El progreso de España en ciberseguridad es bueno y tenemos la oportunidad de posicionarnos como referente"

JOSÉ SEARA
Fundador y consejero delegado de DeNexus

"Para trasladar la importancia de la ciberseguridad a los directivos, es clave hablar su idioma de negocio"

CARLOS PELEGRÍN
Socio de Corporate Learning Solutions de Esade

"La nueva directiva cambia mucho las cosas para los directivos y consejos de administración"

MARGARITA FDEZ. DE PRADA
Directora de transformación digital de Iberdrola

"La digitalización es una ventaja pero también nos hace más vulnerables ante potenciales ciberataques"

Las principales novedades que introduce la normativa

Tras su entrada en vigor en el pasado mes de diciembre, la directiva NIS2 deberá ser transpuesta a la legislación nacional antes del 17 de octubre de 2024. Con el fin de garantizar un alto nivel de ciberseguridad en el conjunto de la UE, introduce la distinción entre dos categorías de entidades afectadas por la normativa: esenciales e importantes. Esta clasificación se basará en el carácter crítico de los sectores en los que actúen, el tipo de servicio que ofrezcan y su tamaño. "Las obligaciones serán idénticas para ambos tipos, pero las sanciones no: la principal diferencia es que las entidades importantes estarán sujetas a un régimen sancionador de menor importe", explicó Jesús Yáñez, socio de cumplimiento normativo, privacidad y ciberseguridad de Ecija.

Con NIS2, los requisitos de seguridad se vuelven más estrictos y las medidas serán proporcionales a los riesgos a los que se encuentra expuesta cada organización. Los Estados miembros deberán garantizar que las entidades ponen en marcha medidas técnicas y organizativas en ámbitos como la seguridad en la cadena de suministro.

Las sanciones también se disparan: si hasta ahora las infracciones más graves se castigaban con cantidades comprendidas entre 500.000 euros y 1 millón, las multas más cuantiosas ascenderán hasta un máximo de al menos 10 millones de euros o un 2% del volumen de negocio anual global para las entidades esenciales. En el caso de las importantes, se trataría de 7,5 millones o un 1,4% de la cifra de negocio. Asimismo, Yáñez advirtió que "los Estados miembros podrán establecer sanciones penales y habrá responsabilidad directa para los altos directivos, e incluso prohibiciones temporales para ejercer cargos".

JESÚS YÁÑEZ
Socio de cumplimiento normativo, privacidad y ciberseguridad de Ecija

"Las entidades importantes estarán sujetas a sanciones más bajas que las esenciales"