LA DIRECTIVA NIS2 ESTABLECE NUEVAS OBLIGACIONES EN MATERIA DE CIBERSEGURIDAD PARA LAS EMPRESAS Y SUS DIRECTIVOS

Madrid, 8 de mayo de 2023 – El pasado 27 de diciembre de 2022, la Unión Europea (UE) lanzó una nueva directiva de seguridad de información de redes, conocida como NIS2, para hacer frente al aumento de los ataques cibernéticos y sus consecuencias en el ámbito empresarial e industrial. Para tratar las implicaciones de la normativa en las organizaciones, EXPANSIÓN y Cipher, el área de ciberseguridad de Prosegur, organizaron el encuentro "El impacto de la normativa NIS2 en los directivos y consejeros".

El encuentro contó con la participación de expertos en ciberseguridad y directivos de grandes compañías referentes en el sector de la tecnología y la ciberseguridad. Durante el evento se debatió sobre las implicaciones de la directiva NIS2 en las empresas y sus directivos, así como los desafíos que esta normativa implica para la adaptación de las organizaciones al creciente número de amenazas que existen en el ámbito de la ciberseguridad.

Javier Cabrerizo, Global Managing director de Prosegur, se encargó de dar la bienvenida a los asistentes del encuentro, y en su intervención declaró el compromiso de Prosegur con la seguridad mundial. "En Prosegur tenemos como misión hacer del mundo un lugar más seguro, desde todas nuestras áreas protegemos familias, hogares y un activo muy importante, el dinero. Además, nuestra actividad se extiende mucho más allá del mundo físico y nuestro trabajo se expande hacia nuevas plataformas, donde entra en juego la ciberseguridad", manifestó.

Jesús Yáñez, Socio de cumplimiento normativo, privacidad y ciberseguridad de Écija Abogados, contextualizó las nuevas implicaciones de la normativa europea NIS2 y el impacto que esta tiene en los Estados miembros de la Unión Europea. Concretamente, afirmó que "Europa ha sido consciente de que la directiva actual de ciberseguridad no es suficiente para la protección de las empresas. El objetivo de la directiva NIS2 es crear una cultura de ciberseguridad".

A continuación, se celebró una mesa de debate en la que participaron algunos de los directivos de grandes compañías referentes en el sector de la tecnología y la ciberseguridad: Carlos Rodríguez Sanz, Líder de Producto de Ciberseguridad Regional APAC y Europa en AXA XL; José Seara, CEO de Denexus; Carlos Pelegrín Fernández López, Socio de Corporate Learning Solutions en ESADE; Margarita Fernández de Prada, Directora de Transformación Digital del Grupo Iberdrola; y David Fernández Granado, director general de Cipher.

Implicaciones de la directiva NIS2 en cada organización

La nueva directiva NIS2 evidencia el esfuerzo de la Unión Europa por adaptarse al creciente número de amenazas en ciberseguridad que existen actualmente. Entre otros aspectos, la directiva NIS2 establece dos nuevas categorías para clasificar a las organizaciones europeas en función de la criticidad en términos de ciberseguridad de su sector, del tipo de servicio que ofrezcan o de su tamaño. Amplía su ámbito de aplicación para sectores que considera esenciales e importantes para la sociedad.

Entre sus aspectos más relevantes, se encuentran la creación de dos nuevas categorías para clasificar a las organizaciones europeas según su criticidad en ciberseguridad, su tipo de servicio o su tamaño, así como la ampliación de su ámbito de aplicación a sectores considerados esenciales e importantes para la sociedad. Además, implica un cumplimiento en cadena, donde tanto las compañías como sus clientes y proveedores deben notificar cualquier incidencia relacionada con la ciberseguridad de su negocio.

David Fernández Granado, director general de Cipher, señala que la NIS2 supone un incentivo para toda la compañía y destaca algunos de los retos que implica la directiva, como la falta de visibilidad en ciberseguridad y la fragmentación tecnológica que afecta a las empresas. Igualmente, destaca la importancia de tener un conocimiento universal de las herramientas necesarias para hacer frente a los retos de este nuevo paradigma. Por otro lado, la falta de talento y la velocidad a la que cambia el sector son otros retos a los que las organizaciones deben enfrentarse. En cuanto a este último, Fernández Granado explica que las organizaciones deben adaptarse al ritmo de crecimiento del sector para que todos los eslabones de la cadena funcionen al mismo nivel.

Por su parte, José Seara, portavoz de Denexus, destaca la necesidad de fomentar la colaboración público-privada para implementar las nuevas tecnologías y coincide con Fernández Granado en que es importante trasladar el desafío de la ciberseguridad a aquellos directivos que no tienen conocimiento de los riesgos para hacer de esta una responsabilidad compartida.

Se espera que la nueva normativa extienda la responsabilidad hacia los directivos de las empresas y, por tanto, se prevé un crecimiento exponencial en la demanda de ciberseguros. Carlos Rodríguez Sanz, de AXA XL, expone que el sector necesita un marco de gobernanza que defina la responsabilidad de cada uno y destaca la importancia de contar con un plan de respuesta ante incidentes y analizar cuidadosamente los contratos con los proveedores, ya que la NIS2 responsabiliza a todos los negocios que forman parte de la cadena de suministro.

Esta responsabilidad en cadena también involucra a las pequeñas y medianas empresas, quienes realizan un trabajo clave y, por lo tanto, deben estar involucradas en las cuestiones de ciberseguridad. David Fernández Granado, asegura que las empresas del sector están haciendo hincapié en la importancia de integrar a las pequeñas y medianas empresas con las que trabajan en las cuestiones relacionadas con la ciberseguridad, pero que aún queda mucho por hacer.

Para hacer frente a los riesgos cibernéticos y asumir las responsabilidades que implica la normativa europea, es fundamental que exista una formación especializada en ciberseguridad en las cúpulas de las empresas. Carlos Pelegrín, de ESADE, destaca la importancia de formar a los directivos de las empresas en materia de ciberseguridad de manera continua y evolutiva, para que puedan estar al día con los avances tecnológicos y las nuevas amenazas. Además, Pelegrín subraya que es esencial que la formación sea práctica y se realicen simulacros y formaciones de manera regular para que los directivos estén preparados para actuar ante cualquier incidencia de seguridad

Claves para posicionar a España en el sector de la ciberseguridad

Margarita Fernández de Prada, directora de Transformación Digital del Grupo Iberdrola, destacó que la nueva directiva NIS2 representa una oportunidad para posicionar a España como un referente en adaptación a las nuevas tecnologías y contribuir a retener el talento en nuestro país. La ejecutiva enfatizó que, aunque la digitalización ofrece ventajas, también aumenta la vulnerabilidad a los ciberataques. Por lo tanto, es importante que las organizaciones y sus consejos consideren estos riesgos y aprovechen la normativa como una oportunidad para asumir la responsabilidad de la seguridad de su empresa.

Finalmente, David Fernández Granado, afirmó que su misión es llevar la seguridad que Prosegur ya proporciona en el mundo físico al mundo digital, identificando los puntos débiles que causan los incidentes cibernéticos. Además, señaló que el 80% de los ataques son llevados a cabo por los mismos actores y se apoyan en vulnerabilidades que surgieron en 2019. Con esto, busca concienciar sobre la importancia de que las empresas adquieran una mayor responsabilidad en cuanto a la ciberseguridad.