Publicado en Madrid el 10/02/2021

El incumplimiento de la nueva normativa de ciberseguridad europea puede tener consecuencias inasumibles

La nueva normativa europea pone de manifiesto la gran importancia de la estrategia de ciberseguridad para la UE y por primera vez establece sanciones para las compañías, en caso de no cumplirlas, "pueden tener un impacto económico devastador para las compañías", según ha anunciado S2 Grupo

Con motivo del refuerzo del marco regulatorio del ámbito de la ciberseguridad por parte de la Unión Europea, la empresa española S2 Grupo ha destacado en un comunicado que esta cuestión "debe ser uno de los ejes de las empresas y es clave adaptarse a la normativa porque, de lo contrario, las consecuencias de una sanción pueden ser inasumibles para los negocios".

Ante la creciente amenaza que plantean los ciberataques, la Unión Europea ha tenido que actualizar la directiva NIS para dotar a los Estados miembros de un marco común que se ha focalizado en la ciberseguridad para garantizar la ciberresiliencia de los procesos que dan soporte a servicios esenciales para la sociedad.

En este sentido, S2 Grupo ha destacado que la nueva estrategia de ciberseguridad de la UE se basa en tres aspectos fundamentales:

- La resiliencia, la soberanía tecnológica y el liderazgo.

- La capacidad operativa para prevenir, disuadir y responder.

- La cooperación para promover un ciberespacio global, seguro y abierto.

“Esta estrategia supone que los Estados miembros deberán transponerla a sus legislaciones nacionales, previsiblemente, 18 meses después de su publicación. Esta revisión de la directiva va a otorgar mayores herramientas de supervisión y ejecución a los controladores, hace especial hincapié en la necesidad de incrementar la ciberseguridad de la cadena de suministro, refuerza la importancia de que la alta dirección de las organizaciones respalde y sean responsables en el cumplimiento de las medidas de ciberseguridad, y mejora la capacidad de intercambio de información entre los distintos actores”, ha explicado José Rosell, socio-director de S2 Grupo.

“Además, la nueva directiva amplía su alcance añadiendo nuevos sectores en función de su importancia para la economía y la sociedad. Y otra novedad importante es el nuevo marco de sanciones que incluye, ya que indica que la no aplicación de medidas de seguridad pueden tener

consecuencias negativas para la ciberresiliencia de las entidades y, por tanto, se debe establecer una lista mínima de sanciones administrativas por incumplimiento de las obligaciones de información y gestión de riesgos de ciberseguridad que sea común en todos los Estados miembros", ha continuado Miguel A. Juan, socio-director de S2 Grupo.

"Ante esta situación, es fundamental que las empresas se conciencien de la importancia de contar con un equipo de expertos en aplicación de ciberseguridad y del cumplimiento de la normativa de ciberseguridad porque, en caso contrario, las consecuencias pueden ser realmente duras para la continuidad de los negocios", ha añadido José Rosell.

"Precisamente, prever que esto sucedería ha sido lo que en 2020 nos llevó a una alianza estratégica de S2 Grupo con el despacho internacional Andersen para poder ofrecer a las compañías una solución real que les permita cumplir con toda la legislación que tiene un fuerte componente tecnológico en materia de ciberserguridad. Así se evita que este asunto decisivo se aborde de forma descoordinada", ha explicado Miguel A. Juan.

Nuevas iniciativas de ciberseguridad en la Unión Europea

Desde S2 Grupo se ha destacado que, en la misma línea de la actualización de la directiva NIS, hay otras dos iniciativas dentro de la nueva estrategia de la UE que son la propuesta de la Comisión del Reglamento para la resiliencia operativa digital del sector financiero (Digital OperationalResilienceAct, DORA) y la propuesta de Directiva sobre resiliencia de las infraestructuras críticas (CIR).

Por lo que se refiere a DORA, es el marco que establece la Comisión Europea para dar un enfoque común sobre la ciberresiliencia del sector financiero. DORA aplica a las entidades de crédito, proveedores de servicios de criptoactivos, proveedores de suministro de datos, empresas de seguridad y reaseguros, fondos de pensiones de empleo, etc. Pero además, los proveedores terceros esenciales de servicios TIC también deben estar muy pendientes de esta normativa, ya que también van a ser objeto de su regulación y supervisión en el marco de la Unión.

Este reglamento regula aspectos como el gobierno de la seguridad, gestión del riesgo, notificación de incidentes, pruebas de resiliencia, riesgos de terceros e intercambio de información.

Junto a esto, S2 Grupo ha resaltado que en España la transposición de la Directiva NIS se realizó mediante el Real Decreto-ley 12/2018, y precisamente acaba de ver la luz, con su publicación en el Boletín Oficial del Estado. Este Real Decreto establece la obligación de definir una estrategia de ciberseguridad que establezca un marco normativo, apoyado en el Esquema Nacional de Seguridad que dote de seguridad jurídica a la estructura de ciberseguridad de las organizaciones y las soluciones tecnológicas que se desplieguen. Además, regula y establece el rol y la responsabilidad del CISO.

Por todo esto, los expertos de S2 Grupo han enfatizado que "ya es más que evidente la gran importancia estratégica de la ciberseguridad a nivel europeo y, por tanto, la adaptación al nuevo marco regulatorio tiene que convertirse en uno de los ejes vertebradores de las compañías".

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Derecho E-Commerce Ciberseguridad