DEBATES ciberseguridad TIC

Construyendo un futuro más seguro con NIS2

IR A PÁGINA SIGUIENTE

Construyendo un futuro más seguro con NIS2

La ciberseguridad se ha convertido en un pilar fundamental para la estabilidad y continuidad de las empresas, especialmente en un contexto donde las amenazas digitales son cada vez más sofisticadas y persistentes. La implementación de la Directiva NIS2 supone un cambio significativo en el marco normativo europeo, con el objetivo de mejorar la resiliencia de las infraestructuras críticas y garantizar la seguridad en sectores esenciales. Sin embargo, su transposición en España ha generado múltiples interrogantes y desafíos que afectan tanto a grandes empresas como a pymes, proveedores tecnológicos y responsables de seguridad.

Rosalía Arroyo

La directiva, que busca reforzar la seguridad de las infraestructuras críticas y mejorar la resiliencia de sectores esenciales, supone un cambio significativo en la forma en que las empresas deben gestionar su ciberseguridad, estableciendo requisitos más estrictos en la gestión del riesgo, la supervisión de proveedores y la notificación de incidentes.

En este contexto, se celebró un debate patrocinado por Mastercard que reunió a representantes de empresas y expertos en ciberseguridad para analizar el impacto de la directiva NIS2 en

las organizaciones, sus desafíos en la implementación y las preocupaciones regulatorias. A lo largo de la sesión, se discutieron los efectos de la transposición de la normativa en España, las dificultades de gestionar la ciberseguridad en la cadena de suministro, la carencia de herramientas adecuadas para su cumplimiento, y el papel que los proveedores tecnológicos pueden jugar en la automatización y optimización de estos procesos.

Un marco normativo con más preguntas que respuestas

El debate comenzó con la intervención de Rafael Hernández González, responsable de proyectos estratégicos de ciberseguridad en Moeve, quien analizó el proceso de transposición de la Directiva NIS2 en España, señalando que, si bien ya se cuenta con un documento de referencia, su aplicación práctica sigue planteando retos. “Contamos con un marco normativo que nos permite avanzar, aunque su implementación en el ámbito empresarial aún requiere mayor concreción”, indicó. Según su visión, la directiva europea ha sido adoptada con un enfoque general, y considera necesario definir con mayor precisión los mecanismos de supervisión y control. “Es fundamental aclarar cómo se van a aplicar las medidas en la práctica, de qué manera se fiscalizarán los controles y cuál será el papel de los supervisores en este proceso”, comentó.

> “La Directiva NIS2 representa un avance importante en la consolidación de la ciberseguridad como un pilar estratégico para las empresas”
>
> **Rafael Hernández González,** responsable de proyectos estratégicos de ciberseguridad en **Moeve**

Uno de los puntos que Rafael Hernández destacó como un área de mejora es la consideración del rol del CISO dentro de la normativa. “El sector ha evolucionado significativamente en los últimos años, pero aún hay aspectos pendientes en cuanto al reconocimiento y posicionamiento del CISO dentro de la estructura de cumplimiento normativo”, reflexionó.

Asimismo, Rafael Hernández planteó la necesidad de encontrar un equilibrio entre la normativa nacional y los estándares internacionales en materia de ciberseguridad, especialmente para empresas con presencia global. “Para aquellas organizaciones que operan en múltiples mercados, resulta clave armonizar los requisitos locales con marcos de referencia internacionales como ISO 27001 o NIST. La adaptación de normativas debe facilitar la integración con estándares ampliamente reconocidos a nivel global”, señaló.

Desde una perspectiva más amplia, Ángel López Zaballos, Cyber Defence Manager en Airbus, quien intervino también como portavoz de la comisión de Ciberseguridad de Ametic, coincidió en que la falta de una transposición homogénea en la Unión Europea es un problema. “Cada país ha interpretado la directiva de forma diferente, y esto genera una serie de disonancias que dificultan la implementación de

> “Cada país ha decidido interpretar la normativa de forma diferente, y esto está generando disonancias en la aplicación de los requisitos”
>
> **Ángel López Zaballos,**
> Cyber Defence Manager en **Airbus**

procesos en grandes empresas, como Airbus”, comentó. En su opinión, el retraso en España puede afectar la competitividad del país, ya que otras naciones que han avanzado más rápido podrían beneficiarse de ello.

Otro punto que destacó Ángel López fue la falta de flexibilidad de la normativa para las pequeñas y medianas empresas. “Las pymes representan la mayor parte del tejido empresarial y no todas tienen capacidad para contratar un CISO a tiempo completo o para desarrollar internamente planes de cumplimiento. Deberíamos apostar por modelos más flexibles, como el uso de CISOs externalizados o servicios compartidos”, propuso.

El reto de la cadena de suministro

Uno de los temas centrales de la discusión fue la creciente preocupación por la ciberseguridad en la cadena de suministro. Luca Lumini, CSO en AXA, explicó que, en su caso, la mayor dificultad radica en la gestión de terceros. “Las medidas técnicas ya las tenemos implantadas, pero lo más complicado es asegurarnos de que nuestros proveedores cumplen con los mismos estándares de seguridad. Al final, la seguridad no sólo depende de lo que hacemos dentro, sino de lo que ocurre fuera”, señaló.

Marina Sanz García, T. Marco normativo en ciberseguridad de Renfe, destacó que su empresa lleva años trabajando en el control de proveedores, pero que ahora están implementando un enfoque más automatizado. “Al ser una empresa pública, nuestras licitaciones ya incluyen requisitos de ciberseguridad, pero ahora estamos trabajando en un modelo de cuestionario automatizado que permita evaluar el nivel de seguridad de los adjudicatarios antes de firmar un contrato”, explicó.

Julio Carriscajo Perez, jefe de ciberinteligencia y análisis en Renfe Operadora, añadió que, en su compañía la preocupación principal es garantizar que solo trabajen con proveedores que cumplan unos mínimos de seguridad. “No queremos encontrarnos con sorpresas una vez que el proveedor ya está trabajando con nosotros. Ahora estamos evaluando soluciones para automatizar la supervisión continua y preventiva y evitar situaciones de riesgo a futuro” comentó.

> “El reto no está solo en lo que hacemos dentro de nuestra organización, sino en garantizar que nuestros proveedores cumplen con los mismos estándares de seguridad”
>
> **Luca Lumini,**
> CSO en **AXA**

Por otro lado, Maite Avelino Carmona, Responsable Ciberseguridad del Ministerio de Defensa, ofreció un enfoque distinto señalando que, aunque su empresa no está directamente sujeta a NIS2, sus proveedores sí lo están. “No podemos ignorarlo sólo porque no se nos aplique directamente. Si atacan a uno de nuestros proveedores, el impacto nos alcanzará de igual manera. Es algo que no se ha considerado lo suficiente en la normativa”, advirtió.

> “En Renfe estamos trabajando en la automatización del proceso para evaluar y supervisar el cumplimiento de nuestros proveedores de manera más eficiente”
>
> **Marina Sanz García,**
> T. Marco normativo en ciberseguridad,
> **Renfe**

Dificultades en la evaluación del cumplimiento y la falta de herramientas

Fernando Sanz de Galdeano Sanz, CISO en Arcano Partners, explicó que la dificultad no radica sólo en cumplir con las diferentes normativas y regulaciones, sino en adaptar el lenguaje a cada supervisor o a cada tipo de revisión. “Nos encontramos con nuevas normativas con respecto a las ya existentes, junto con revisiones y auditorías que nos exigen clientes y terceros... y el problema real no es demostrar el cumplimiento, sino entender el alcance y adaptar el ámbito de un mismo control evaluado según el supervisor, el reglamento, o el foco de la auditoría. Algunos reglamentos se solapan y no está claro cómo se va a orquestar todo esto, dado que no hay un marco único de evaluación de controles homogéneo para todas las partes”, afirmó.

Alfonso Martínez, responsable ciberseguridad en una empresa confidencial, coincidió en que la falta de una taxonomía clara de riesgos complica la gestión de la ciberseguridad en las organizaciones. “En muchas empresas, el ciberriesgo sigue estando dentro del riesgo operacional, cuando en realidad debería considerarse como un riesgo independiente. Hasta que no se entienda esto, seguirá siendo difícil justificar inversiones en seguridad”, comentó.

> “La gestión del riesgo en la cadena de suministro es una prioridad para nosotros”
>
> **Julio Carriscajo Pérez,**
> Jefe de ciberinteligencia y análisis en
> **Renfe Operadora**

Juan Rodríguez, regional director de Mastercard, explicó que su compañía está desarrollando soluciones para facilitar el cumplimiento normativo, ofreciendo una visión más clara de los riesgos. “Estamos trabajando en herramientas que permitan mapear diferentes normativas como NIST, ISO 27001 y ENS, de manera que las empresas puedan visualizar de forma sencilla su nivel de cumplimiento y tomar decisiones informadas”, explicó.

Retorno de la inversión en seguridad

El debate también incluyó una reflexión sobre el papel de los ciberseguros en la estrategia de ciberseguridad de las empresas. Maite Avelino Carmona señaló que, si bien los seguros pueden ser una herramienta útil dentro de una estrategia de mitigación de riesgos, no siempre ofrecen cobertura integral frente a todas las consecuencias de un incidente. En particular, destacó que aspectos como el daño reputacional y el lucro cesante pueden no estar suficientemente contemplados en algunas pólizas. "Es importante entender que un ciberseguro no debe ser la única medida de protección. Ha habido casos en los que, a pesar de contar con seguros, las organizaciones han seguido enfrentando dificultades tras un incidente de seguridad", explicó.

> "Aunque nuestra empresa no está directamente sujeta a NIS2, nuestros proveedores sí lo están. No podemos ignorar los riesgos en la cadena de suministro porque cualquier brecha de seguridad en un tercero puede afectarnos de forma directa"

Maite Avelino Carmona,
Responsable Ciberseguridad del
Ministerio de Defensa

Por su parte, Ángel López Zaballos, comentó que en muchas empresas existe la tendencia a optar por seguros en lugar de invertir en medidas preventivas, principalmente porque resulta más sencillo justificarlo ante la alta dirección. "Desde una perspectiva financiera, un seguro es una inversión tangible y cuantificable, mientras que la ciberseguridad a menudo se percibe como un gasto sin retorno inmediato. Sin embargo, la experiencia demuestra que, a largo plazo, la prevención y la protección activa suelen ser más rentables y efectivas", subrayó.

> "El problema no es solo cumplir con la regulación, sino demostrarlo. Nos enfrentamos a una avalancha de regulaciones y la supervisión de controles se ha convertido en una carga operativa importante para los distintos equipos técnicos, en ausencia de un marco único de control"

Fernando Sanz de Galdeano Sanz,
CISO en **Arcano Partners**

Juan Rodríguez explicó que Mastercard está desarrollando herramientas que permitan cuantificar el impacto financiero de los ciberataques y demostrar el retorno de inversión en seguridad.

"Muchas empresas prefieren pagar después del incidente en lugar de invertir en prevención. Nuestro objetivo es ayudarles a entender el coste real de no protegerse", concluyó.

Conclusión: Un Marco Normativo en Evolución y Desafíos por Resolver

El debate dejó en evidencia que la transposición de la Directiva NIS2 en España supone un avance significativo en la consolidación de la ciberseguridad como un aspecto prioritario para las organizaciones. No obstante, su implementación presenta desafíos que requieren un enfoque coordinado entre el sector público y privado.

Uno de los principales puntos destacados fue la necesidad de mayor claridad en la aplicación de la normativa, especialmente en lo que respecta a la supervisión de los controles, la responsabilidad de los actores implicados y la alineación con marcos normativos internacionales. En este sentido, se subrayó la importancia de encontrar un equilibrio entre el cumplimiento regulatorio y la viabilidad operativa para las empresas, evitando una carga administrativa excesiva que pueda dificultar la adopción de medidas efectivas de ciberseguridad.

> "Es fundamental que las empresas evolucionen hacia un enfoque en el que la seguridad digital sea un pilar central, con métricas claras y una evaluación de impacto que permita tomar decisiones informadas y alineadas con los objetivos del negocio"
>
> **Alfonso Martínez,**
> responsable de Ciberseguridad en una empresa confidencial

Otro aspecto clave abordado fue el impacto en la cadena de suministro. La normativa exige a las organizaciones un mayor control sobre la seguridad de sus proveedores, lo que representa un reto significativo en términos de supervisión y evaluación del cumplimiento. Se coincidió en que la automatización de estos procesos puede ser una solución clave para facilitar la gestión del riesgo sin comprometer la eficiencia operativa.

Asimismo, se discutió el papel del CISO dentro de la nueva regulación, resaltando la importancia de fortalecer su rol en la toma de decisiones estratégicas y asegurar que cuente con el respaldo necesario para desempeñar su función de manera efectiva.

En relación con la inversión en seguridad, se destacó que muchas empresas siguen percibiendo la ciberseguridad como un gasto en lugar de una inversión estratégica. Se insistió en la necesidad de cambiar esta mentalidad y considerar la seguridad como un factor clave para la continuidad del negocio y la protección de los activos digitales.

Por último, el debate también puso de manifiesto la relevancia de los ciberseguros como complemento dentro de una estrategia integral de ciberseguridad. No obstante, se enfatizó que estos no deben sustituir las medidas preventivas ni la adopción de buenas prácticas de seguridad.

En definitiva, la implementación de NIS2 abre una nueva etapa en la gestión de la ciberseguridad en España y en la Unión Europea. Si bien todavía quedan incógnitas por resolver, el proceso de adaptación debe verse como una oportunidad para fortalecer la resiliencia de las organizaciones y avanzar hacia un entorno digital más seguro y preparado para los desafíos del futuro.

> “En Mastercard estamos desarrollando soluciones que integran inteligencia artificial para mapear normativas como NIS2, NIST e ISO 27001, facilitando la supervisión y reduciendo la carga operativa para los equipos de ciberseguridad”

Juan Rodríguez,
regional director de **Mastercard**

Barómetro

Descubra todo lo que necesita saber sobre la normativa NIS2 y su impacto en su organización. Este informe, elaborado por TAI Editorial en colaboración con Mastercard, describe los requisitos clave, define quiénes se ven afectados y analiza la preparación de las organizaciones para esta normativa.

EL INFORME ESTÁ DISPONIBLE EN INGLÉS Y ESPAÑOL