OBSERVATORIO TAI **NIS2**

NIS2: un escudo de seguridad para la era digital

IR A PÁGINA SIGUIENTE

Observatorio TAI - NIS2

Igual que los debates, talleres o almuerzos ejecutivos, Observatorio TAI es una más de las acciones que llevamos a cabo en TAI Editorial. Dicho así parece fácil, pero es, con diferencia, la actividad más compleja. Primero, porque se desarrolla a lo largo de varios meses; segunda, porque requiere la colaboración de mucha gente, no sólo del propio Grupo TAI, sino del sector sobre el que impacta que, en este caso, ha sido el de ciberseguridad.

Es un proyecto largo que ha conllevado la publicación de dos revistas digitales y la elaboración de un estudio a partir de las respuestas de más de 100 profesionales españoles que han dedicado un rato de su tiempo, algo escaso en este frenético mundo cíber, para poner sobre la mesa cómo se está abordando la adopción de la Directiva NIS2 (Network and Information Systems) elaborada por la Unión Europea para garantizar un alto nivel común de ciberseguridad en todo el territorio.

Este Observatorio, el primero, ha sido un proyecto largo que se ha abordado con muchísima ilusión y que en gran medida ha sido impulsado por Santiago Campuzano, responsable de Veeam en la región de Iberia, y Ángel Porras, director de desarrollo del Grupo Tai. Gracias a ambos.

Y gracias a todos lo que respondisteis a nuestras preguntas, y a los que nos acompañasteis a la presentación de los resultados del estudio, donde también pudimos contar con la colaboración de Javier Carvajal, CEO y socio fundador de Icraitas, que arrojó luz y dio sentido a las cifras y gráficos del estudio. Gracias también a él.

Y gracias a todos los que dedicasteis un rato a responder la encuesta, y el cuestionario, y a los compañeros que estuvieron pendientes de grabar, maquetar, convocar y organizar. En definitiva; gracias a la valiosa contribución de cada uno, este primer Observatorio TAI ha sido un rotundo éxito.

Barómetro NIS2

PATROCINADORES

Entidad colaboradora

Introducción

NIS2 es la Directiva Europea de Ciberseguridad más compleja que se ha formalizado hasta la fecha. Se presenta como un marco integral que tiene como objetivo fortalecer significativamente la protección de los sistemas de información y redes en toda la Unión Europea en un amplio conjunto de industrias y sectores, con la exigencia de implantar unas medidas mínimas de protección.

Una directiva, que actualiza la anterior (NIS), absolutamente necesaria para adaptarse al nuevo paradigma del mercado de la ciberseguridad que ha evolucionado en temas tan críticos como el crecimiento en el volumen de los ciberataques complejos, con el *ransomware* a la cabeza de los mismos. Un panorama de amenazas que exige una postura de seguridad diferente: ya no solo se trata de evitar el ataque, sino de contar con capacidad de respuesta, tanto para la remediación como para reportar la brecha de seguridad y dar continuidad al estado de la incidencia. Por último, la rápida evolución del mercado exige una normativa que se adapte también a los cambios que se suceden.

Pero no sólo establece requisitos más estrictos para garantizar un alto nivel común de ciberseguridad en todos los Estados miembros, sino que incluye un mayor número de sectores y empresas consideradas esenciales. Además, NIS2 define con mayor precisión las obligaciones de las empresas, como la gestión de riesgos, la notificación de incidentes y la realización de pruebas de intrusión.

La normativa impone una serie de obligaciones a las empresas afectadas como la necesidad de que identifiquen, evalúen y gestionen los ciberriesgos a los que están expuestas. Para ello, deben implementar medidas de seguridad adecuadas capaces de proteger sus sistemas y datos. No sólo están obligadas a notificar a las autoridades competentes cualquier incidente de ciberseguridad que pueda tener un impacto significativo sino que deben contar con planes para restaurar sus sistemas y servicios en caso de un ciberataque.

¿A quién aplica la NIS2?

Un avance clave en la NIS2 es la clasificación de las entidades en dos categorías: “esenciales” e “importantes”. Esta distinción afecta al al-

cance de la directiva y a las implicaciones para los diferentes tipos de organizaciones.

La categoría de **entidades esenciales**, también reconocida por la NIS, abarca sectores fundamentales para el bienestar social y económico.

- **Energía.** Las empresas del sector energético, como las compañías eléctricas, las de gas y las de generación de energía renovable son especialmente vulnerables a los ciberataques. NIS2 impone requisitos estrictos para proteger sus sistemas de control industrial y garantizar la continuidad del suministro.
- **Transporte.** El sector del transporte, incluyendo el aéreo, marítimo y terrestre, también se encuentra en el punto de mira de NIS2. La protección de sistemas de control de tráfico aéreo, puertos y redes ferroviarias es fundamental para evitar interrupciones y riesgos para la seguridad.
- **Salud.** Las instituciones sanitarias, hospitales y proveedores de servicios de salud deben cumplir con requisitos específicos para proteger los datos de los pacientes y garantizar la continuidad de los servicios médicos.
- **Servicios financieros.** Los bancos, las aseguradoras y otras instituciones financieras son objetivos constantes de los cibercriminales. NIS2 obliga a estas entidades a reforzar sus medidas de seguridad para proteger los datos financieros de sus clientes. También están cubiertas por la Ley DORA.

> La directiva permite a las empresas elegir las medidas de seguridad más adecuadas para su entorno

- **Agua.** La gestión del agua es un servicio esencial y, por lo tanto, está sujeto a los requisitos de NIS2. La protección de las infraestructuras hídricas es crucial para garantizar el suministro de agua potable.
- **Infraestructura digital.** Incluye puntos de intercambio de Internet, proveedores de servicios DNS y centros de datos.
- **Administración pública.**

Son los más afectados por la normativa porque son considerados infraestructuras críticas, lo que significa que un ciberataque puede tener un impacto significativo en la sociedad y la economía. Además, gestionan grandes volúmenes de datos sensibles, como información personal, financiera y de salud. Sus sistemas son complejos y están interconectados, lo que los hace más vulnerables a los ataques.

Para estas entidades, NIS2 reafirma su estado crítico e incrementa los requisitos de cumplimiento. Por ejemplo, la notificación de incidentes

> Una de las herramientas claves para asegurar el cumplimiento de cualquier normativa, incluida NIS2, son las sanciones económicas

debe producirse en un plazo de 24 horas, lo que supone una actualización importante con respecto a la directiva anterior.

Las **"entidades importantes"**, por su parte, suponen una adición a la NIS2. Agrupa a los servicios postales y de mensajería, fabricación de determinados productos críticos (productos farmacéuticos, químicos y dispositivos médicos), gestión de residuos, infraestructura espacial terrestre, investigación, servicios digitales (plataformas de redes sociales, mercados en línea y motores de búsqueda), producción, procesamiento y distribución de alimentos, redes o servicios de comunicaciones electrónicas; y proveedores de servicios digitales (servicios de computación en la nube, red de entrega de contenido (CDN), proveedores de servicios gestionados y proveedores de servicios de seguridad gestionados).

Medidas técnicas y organizativas exigidas por NIS2

La Directiva NIS2 establece un marco de ciberseguridad robusto, imponiendo a las empresas una serie de medidas técnicas y organizativas para proteger sus sistemas y datos. Estas medidas varían según el tamaño de la empresa y la criticidad de los servicios que presta, pero en general se centran en los siguientes aspectos:

Medidas técnicas

- **Gestión de identidades y accesos (IAM).** Implementación de sistemas sólidos de autenticación y autorización para controlar el acceso a los sistemas y datos.
- **Cifrado.** Protección de los datos en reposo y en tránsito mediante técnicas de cifrado robustas.
- **Protección perimetral.** Uso de *firewalls*, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para proteger la red de acceso no autorizado.
- **Controles de acceso a la red.** Segmentación de la red para limitar el movimiento lateral de un atacante en caso de una brecha.
- **Software seguro.** Uso de software actualizado y libre de vulnerabilidades conocidas.
- **Copia de seguridad y recuperación.** Implementación de procedimientos regulares de copia de seguridad y planes de recuperación ante desastres.
- **Continuidad del negocio.** Desarrollo de planes para mantener los servicios esenciales en caso de un incidente de ciberseguridad.

Medidas organizativas

- **Gestión de riesgos.** Realización de evaluaciones de riesgos periódicas para identificar y mitigar las amenazas.
- **Política de seguridad de la información.** Desarrollo y comunicación de una política de seguridad de la información que establezca los requisitos de seguridad para todos los empleados.
- **Conciencia y formación.** Impartición de formación a los empleados sobre seguridad de la información y concienciación sobre las amenazas cibernéticas.
- **Gestión de incidentes.** Establecimiento de procedimientos para la detección, respuesta y notificación de incidentes de seguridad.
- **Continuidad del negocio.** Desarrollo de planes para mantener los servicios esenciales en caso de un incidente de ciberseguridad.
- **Terceros.** Gestión de riesgos asociados a terceros, como proveedores y socios comerciales.
- **Divulgación coordinada de vulnerabilidades.** Participación en programas de divulgación coordinada de vulnerabilidades para garantizar la corrección de las vulnerabilidades de forma segura.

Las medidas de seguridad no sólo deben ser proporcionales al tamaño de la empresa y al riesgo al que está expuesta, sino que la directiva permite a las empresas elegir las medidas de seguridad más adecuadas para su entorno específico. Las empresas deben garantizar

> Son consideradas infraestructuras críticas cuando un ciberataque puede tener un impacto significativo en la sociedad y la economía

la continuidad de sus servicios esenciales en caso de un incidente de ciberseguridad.

Queda claro que NIS2 exige a las empresas adoptar un enfoque proactivo y holístico de la seguridad de la información, y que las medidas técnicas y organizativas deben integrarse en todos los aspectos de la empresa, desde la tecnología hasta los procesos y la cultura organizacional.

Multas: un incentivo para la ciberseguridad

Una de las herramientas claves para asegurar el cumplimiento de cualquier normativa, incluida NIS2, son las sanciones económicas. Las multas impuestas por NIS2 pueden ser significativas y varían en función de la gravedad de la infracción y el tamaño de la empresa.

Tanto las entidades esenciales como las importantes tienen idéntica obligatoriedad en el cumplimiento de la directiva. La única distinción hace referencia a las cuantías de penalización en el caso de un in-

cumplimiento: las sanciones son de hasta 10 millones de euros o un máximo de un 2 % del volumen de negocio anual en el caso de las entidades esenciales; o de hasta 7 millones de euros o un máximo de un 1,4 % de la facturación en el caso de las entidades importantes. En casos graves de incumplimiento, las autoridades pueden suspender temporalmente la prestación de servicios.

Además, en función de la gravedad de la infracción o del tamaño de la empresa, la cuantía de la multa depende del sector al que pertenezca, que hayan sido sancionadas anteriormente por incumplir la normativa o que se coopere con las autoridades durante la investigación de una infracción, en cuyo caso la sanción será menor.

La directiva especifica que la alta dirección de la empresa debe supervisar la gestión de riesgos de ciberseguridad y que, junto con el consejo de administración, puede ser considerado, personalmente, responsables del incumplimiento de las obligaciones de la directiva. Es decir, la responsabilidad ya no solo recae en la empresa, sino que en determinadas ocasiones puede tener, incluso, una repercusión a nivel personal.

Encuesta en España

Tomar el pulso al mercado, saber qué desafíos están afrontando las empresas españolas a la hora de hacer frente a la normativa o qué mecanismos están implementando para tener control sobre la cadena

de suministro ha sido el objetivo de una encuesta realizada a más de cien empresas españolas de diferentes tamaños y sectores.

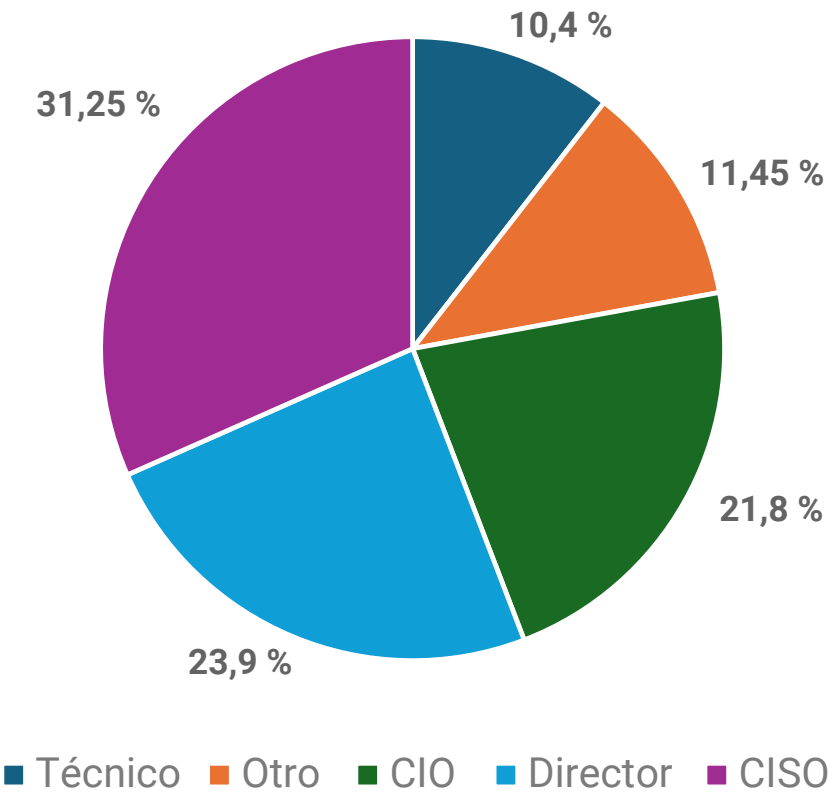
Destaca la participación de la figura del CISO, con un 31,25 % del total, seguida de la del director, con un 23,9 %.

En cuanto al tamaño de empresas, el estudio refleja la casuística del mercado español, con un alto porcentaje de pequeñas y medianas empresas, lo que lleva a dar más valor al alto porcentaje de participación en el estudio de empresas de más de 5.000 empleados (23,9 %), frente a las empresas de entre 501 a 1.000 (11,4 %), o de 1.001 a 5.000 (18,75 %).

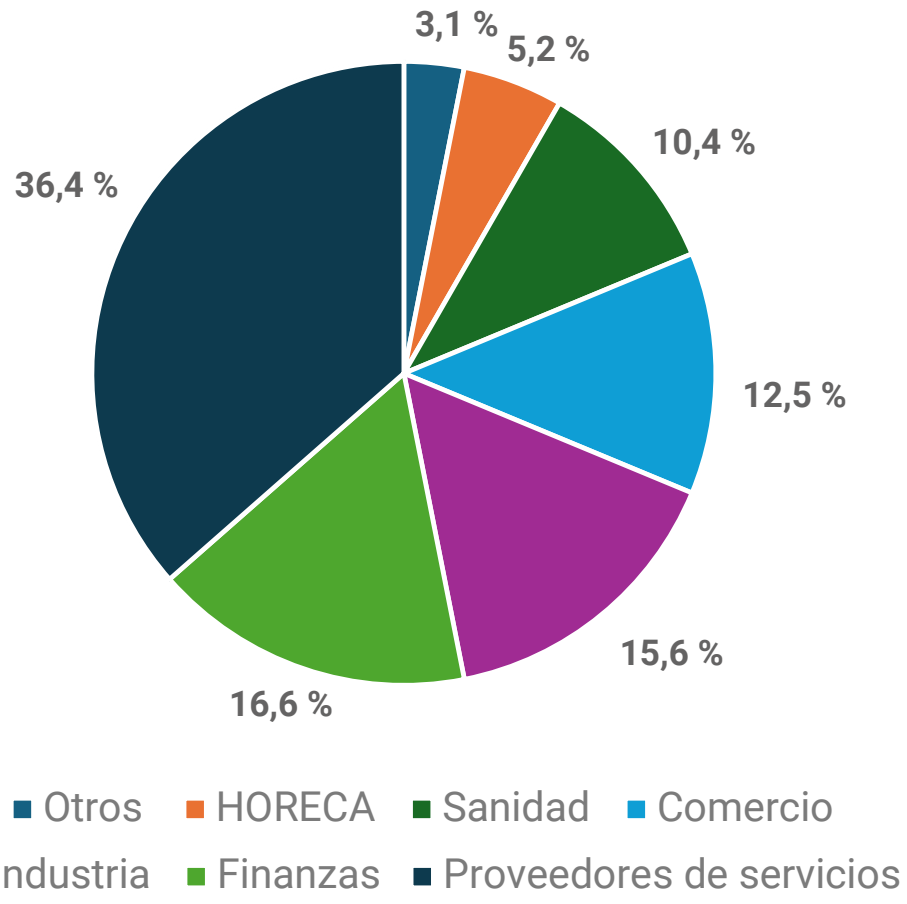
En cuanto los sectores de actividad de las empresas encuestadas, los proveedores de servicios son los más participativos, con un 36,4 % de total, seguido de finanzas (16,6 %), industria (15,6 %) y comercio (12,5 %).

Tipología de la muestra

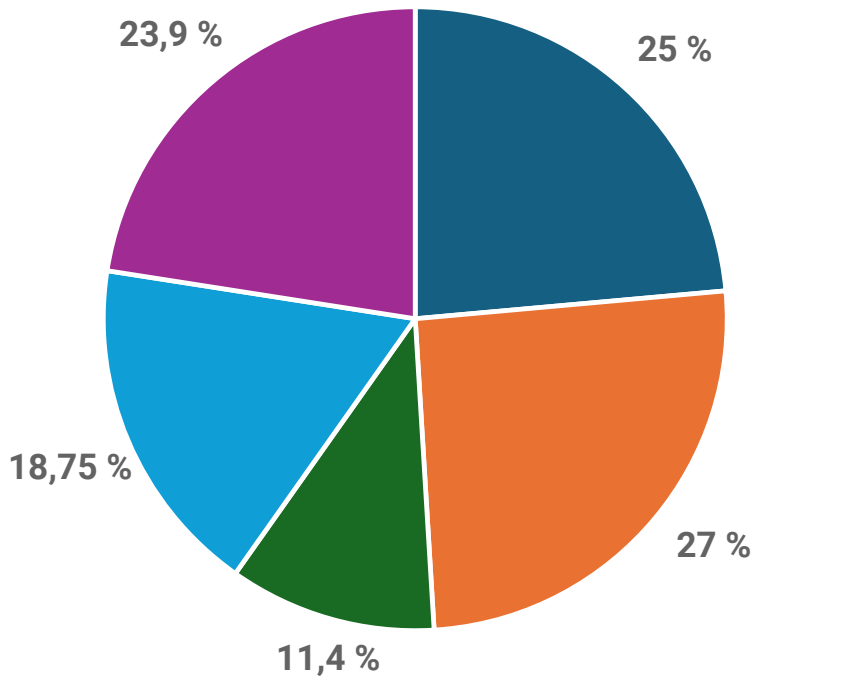
Perfil encuestados



Sector de actividad

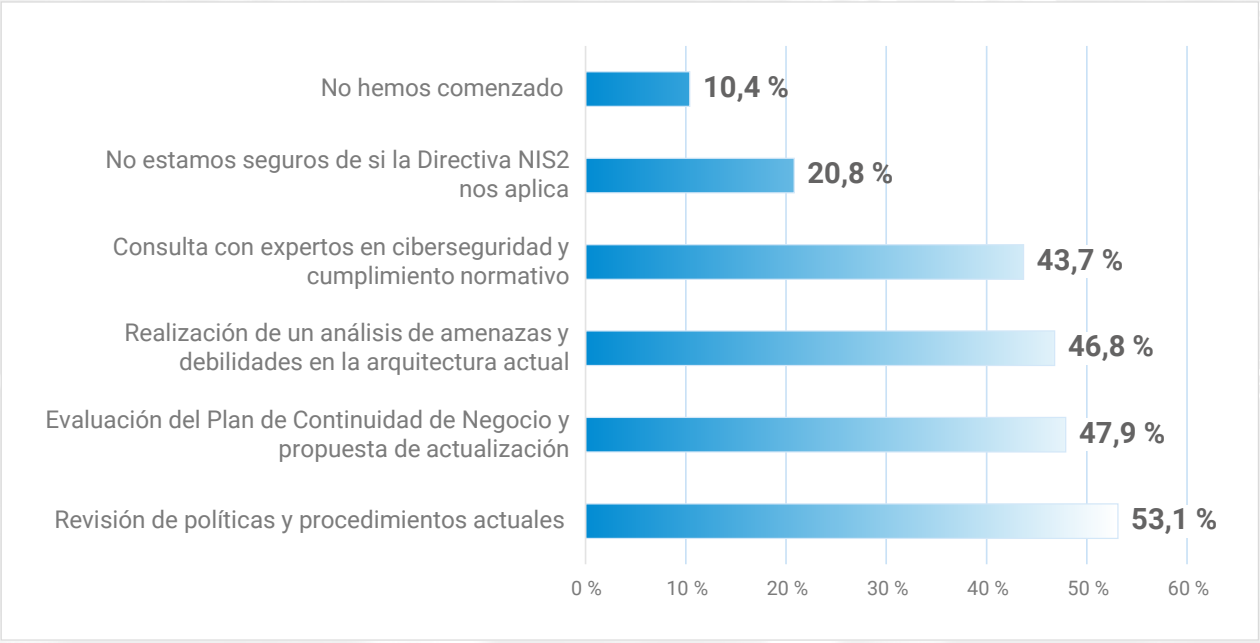


Tamaño de empresa



Resultados del estudio

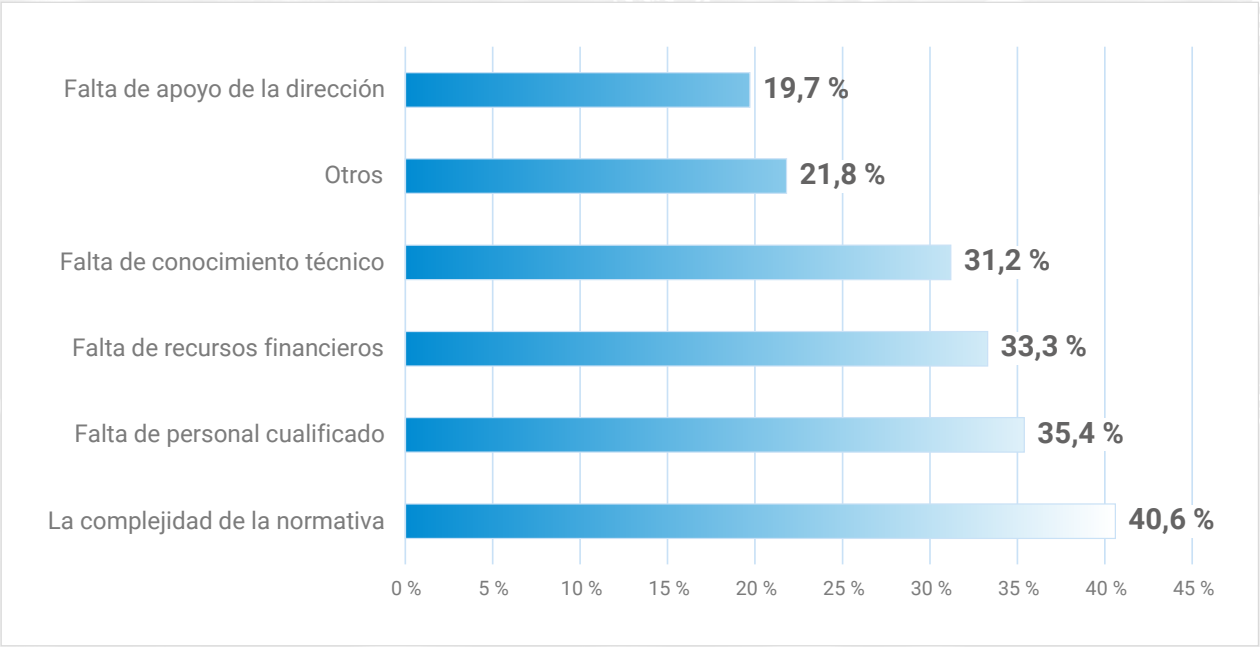
¿Qué pasos ha tomado para realizar una evaluación inicial del cumplimiento de NIS2 en su empresa?



Antes de implementar una directiva hay que identificar si una organización está dentro del ámbito de aplicación de la misma, por lo que es fundamental llevar a cabo una evaluación. Existe una gran disparidad entre las empresas en cuanto a su nivel de preparación para cumplir con NIS2. Mientras que algunas han tomado medidas, otras (10,4 %) aún no han tomado ninguna, lo que **sugiere una falta de conciencia** o comprensión de la importancia de esta directiva y de las implicaciones que puede tener para sus operaciones.

Las empresas que han iniciado el proceso de evaluación se han centrado principalmente en áreas como la revisión de políticas y procedimientos (53,1 %), la evaluación del **plan de continuidad del negocio** (47,9 %) o el análisis de amenazas y habilidades (46,8 %), lo que indica que reconocen la importancia de estas áreas para cumplir con los requisitos de NIS2.

¿Cuáles son los principales desafíos que enfrenta su empresa para cumplir con la Directiva NIS2?

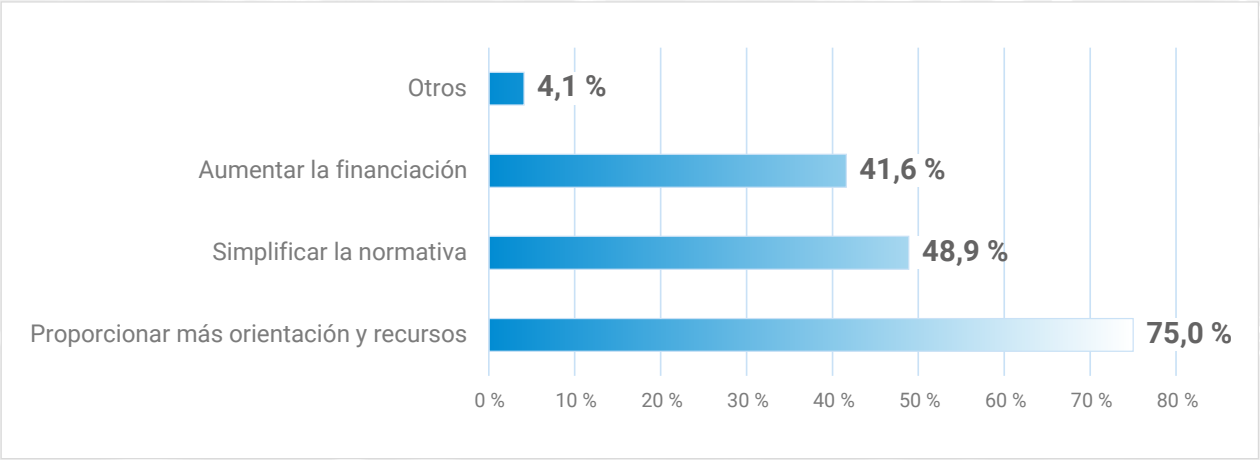


La **complejidad** de la normativa NIS2 se erige, para el 40,6 % de los encuestados, como el desafío más significativo.

Las múltiples disposiciones, requisitos técnicos y legales, así como las constantes actualizaciones, dificultan su interpretación y aplicación. Esta complejidad, que ralentiza los procesos de implementación y aumenta el riesgo de errores en la interpretación y en la aplicación de las medidas de seguridad, se suma a la **falta de personal cualificado** (35,4 %) y de conocimientos técnicos de la misma (31,2 %).

La falta de apoyo por parte de la dirección es para el 19,7 % de los encuestados un desafío a la hora de cumplir con NIS2.

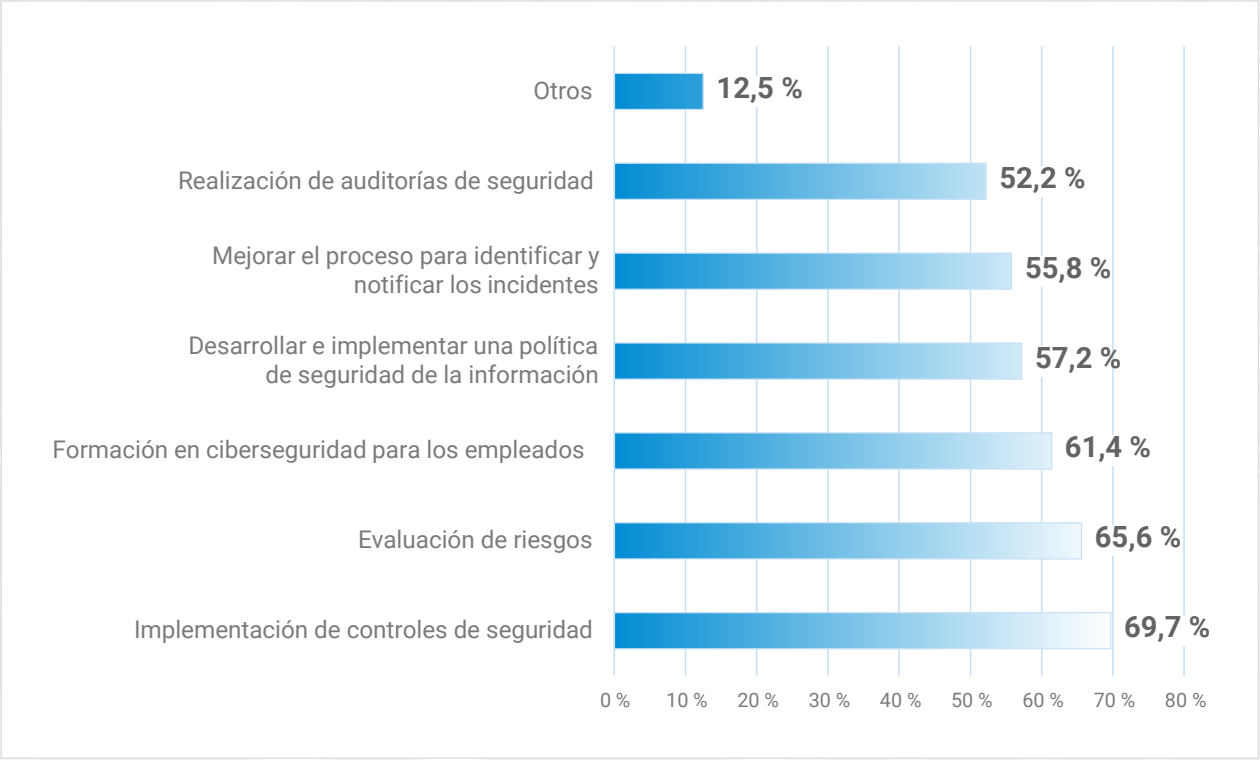
¿Qué medidas cree que las autoridades podrían tomar para facilitar la implementación de la Directiva NIS2 por parte de las empresas?



Siempre es un reto implementar una nueva reglamentación y son muchos los directivos a los que les gustaría contar con una mayor ayuda en la implementación de NIS2.
A partir de los datos de la encuesta podemos extraer las siguientes conclusiones:

- **Necesidad de un mayor apoyo institucional.** Las empresas demandan activamente una mayor orientación y recursos por parte de las autoridades para implementar la Directiva NIS2.
- **Complejidad de la normativa.** Su complejidad se percibe como un obstáculo significativo para su implementación.
- **Falta de recursos.** Muchas empresas carecen de los recursos necesarios (tanto económicos como humanos) para cumplir con los requisitos de NIS2.

¿Qué medidas ha tomado su empresa para aumentar su ciberseguridad y prepararse para NIS2 en el último año?



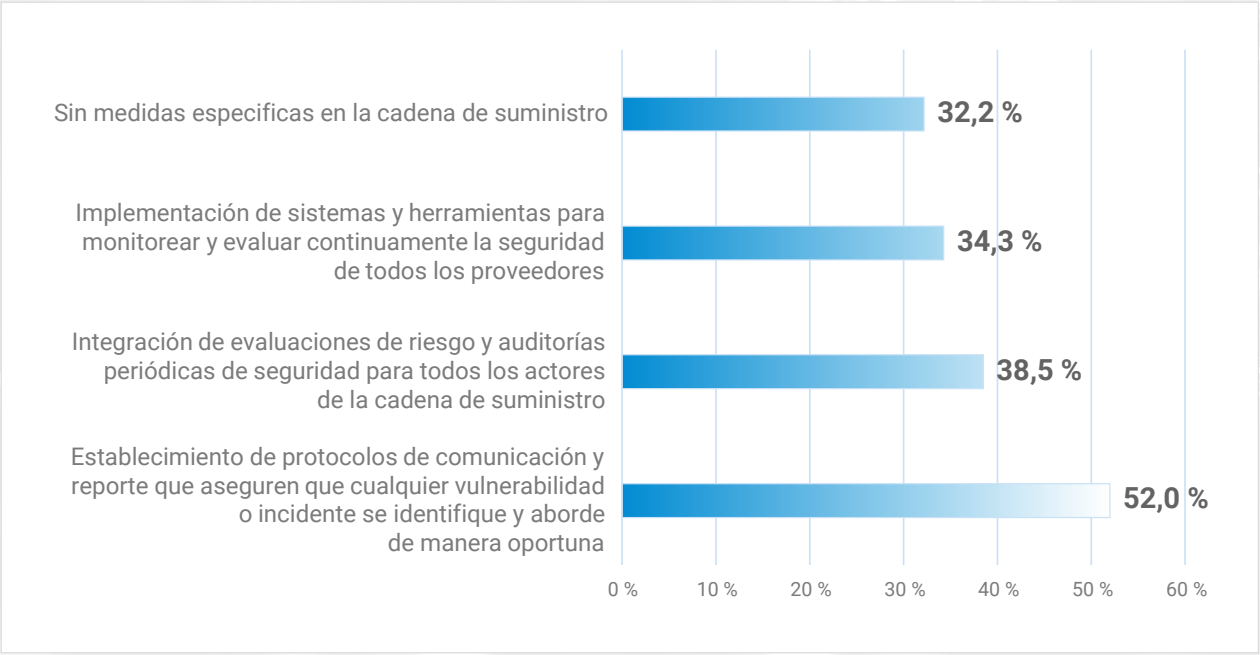
La implementación de **controles de seguridad**, adoptada por el 69,7 % de las empresas, es la medida más ampliamente adoptada, lo que indica un esfuerzo por proteger los sistemas y datos de la empresa.

También se reconocen la importancia de identificar y evaluar los **riesgos de seguridad** (65,6 %) de forma proactiva, lo que demuestra una comprensión clara de que la seguridad comienza por conocer las amenazas potenciales.

La ciberseguridad es una responsabilidad de todos los empleados y el 61,4 % de las compañías está invirtiendo en formación para concienciar y capacitar a su personal.

Por la mejora en la **gestión de incidentes** también apuestan el 55,8 % de las empresas para detectar, responder y notificar incidentes de seguridad de manera más eficiente.

¿Qué mecanismos ha implementado para garantizar una visibilidad completa y continua de la seguridad en toda su cadena de suministro?



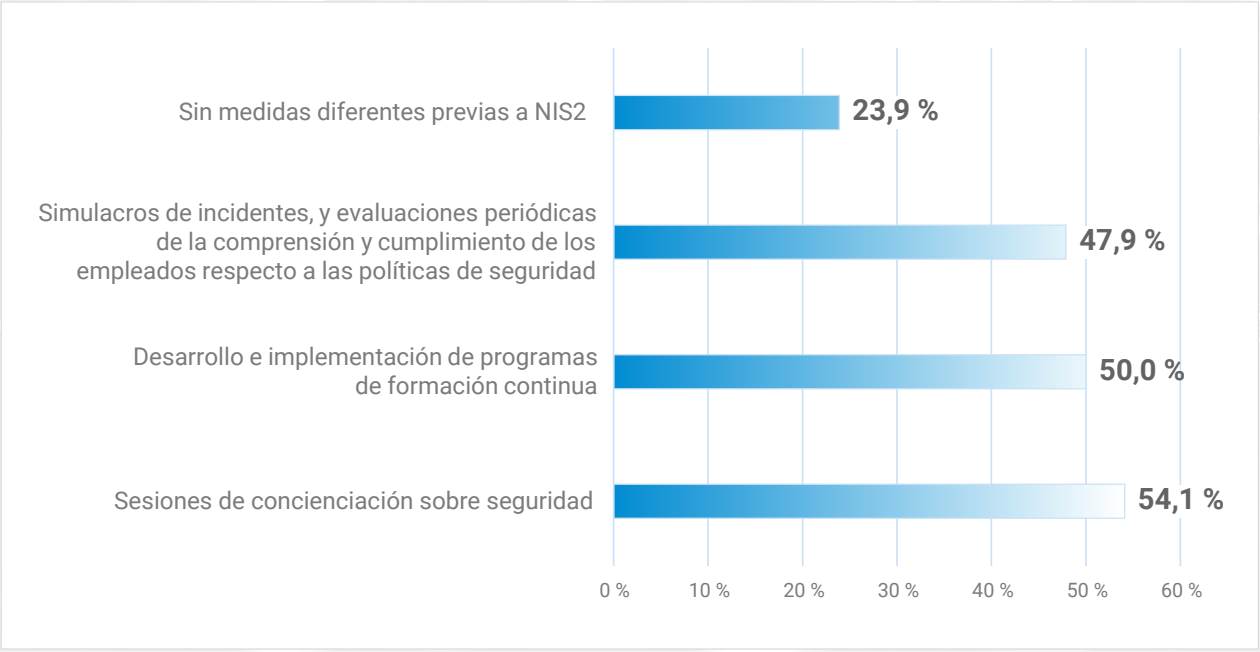
Una **visibilidad completa y continua en la cadena de suministro** protege a la empresa contra riesgos y amenazas, mejora su eficiencia, cumplimiento normativo y reputación.

Los datos de la encuesta muestran que el 52 % de las empresas reconoce la importancia de establecer canales de comunicación claros y eficientes para identificar y responder a incidentes de seguridad en toda la cadena de suministro.

La realización de **evaluaciones de riesgo y auditorías de seguridad** (38,5 %) a todos los proveedores demuestra un enfoque proactivo para identificar y mitigar las vulnerabilidades.

Por otra parte, un porcentaje significativo de empresas (32,2 %) **aún no cuenta con medidas específicas** para garantizar la visibilidad en su cadena de suministro, lo que representa un área de mejora.

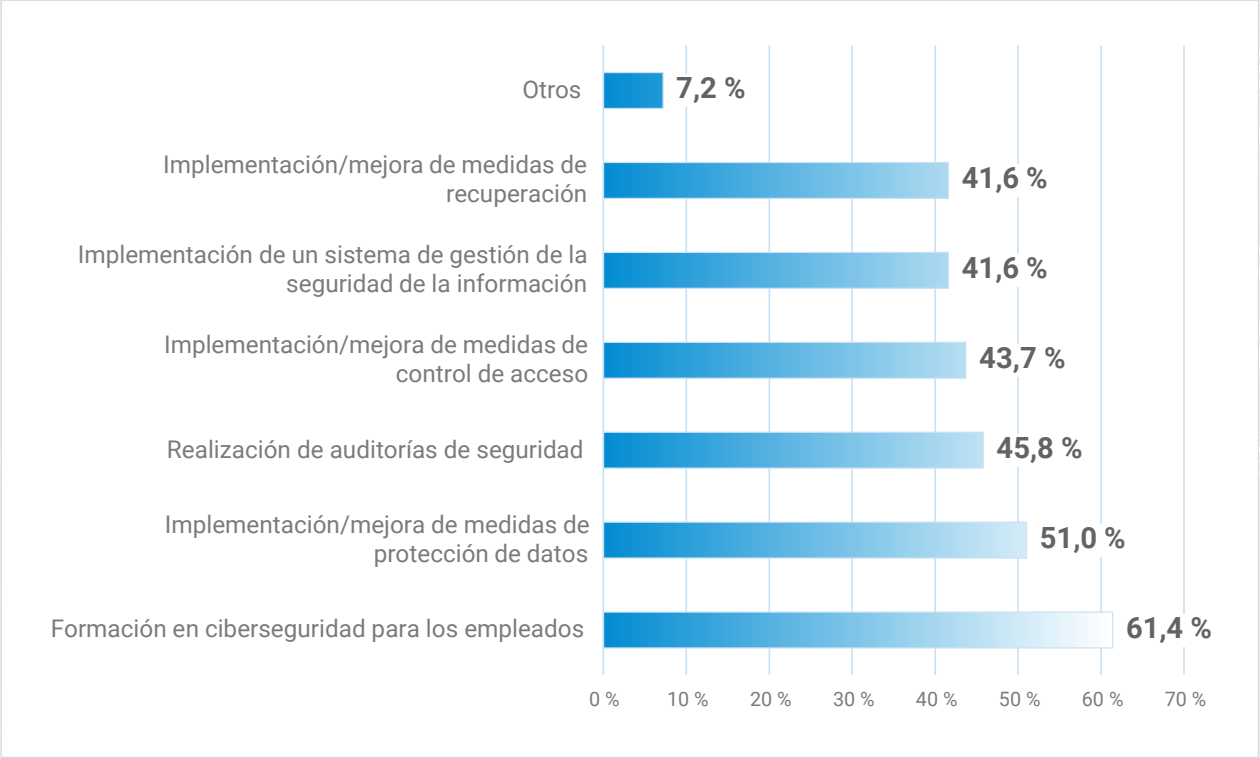
¿Cómo asegura la capacitación y concienciación de los empleados sobre las obligaciones y medidas de seguridad bajo NIS2?



Invertir en la **capacitación y concienciación** de los empleados fortalece la capacidad de la empresa para prevenir, resistir y recuperarse de incidentes de ciberseguridad.

Aunque casi un 24 % de las compañías reconoce no llevar a cabo medidas diferentes previas a la NIS2, lo que indica que hay margen para mejorar, entre el 48 % y el 54 % se apoya en sesiones de concienciación sobre seguridad, en el desarrollo e implementación de programas de **formación continua y en simulacros de incidentes** y evaluaciones periódicas de la comprensión y cumplimientos de los empleados respecto a las políticas de seguridad.

¿En qué ámbitos planea focalizarse su empresa para aumentar su ciberseguridad en el próximo año?



La **formación** de los empleados en ciberseguridad vuelve a ser un aspecto importante, esta vez para el 61,4 % de las empresas que tiene claro el papel crucial que desempeña el factor humano en la prevención de incidentes.

La **protección de los datos** se ha convertido en una prioridad absoluta: el 51 % de las organizaciones quiere llevar a cabo la implementación o mejora de medidas de protección.

Las empresas están adoptando un **enfoque integral de la ciberseguridad**, combinando diversas medidas como auditorías (45,8%), control de acceso (43,7 %) y planes de recuperación (41,6 %). Esto indica una comprensión más profunda de la complejidad de las ciberamenazas y la necesidad de una defensa en capas.

Sumario ejecutivo

En conclusión, los resultados de la encuesta ponen de manifiesto la necesidad de una mayor concienciación y acción por parte de las empresas para cumplir con NIS2. Aquellas que no tomen las medidas necesarias se exponen a riesgos significativos, como multas económicas y daños a su reputación.

Los desafíos para cumplir con NIS2 son múltiples y complejos. Sin embargo, las empresas que tomen medidas proactivas para abordar estos desafíos podrán mejorar su postura de seguridad y proteger sus activos.

Las empresas están tomando medidas importantes para mejorar su ciberseguridad y prepararse para NIS2. Sin embargo, es fundamental que estas medidas se implementen de forma integral y se adapten a las necesidades específicas de cada organización. Además, es necesario realizar un seguimiento continuo de la eficacia de estas medidas y realizar ajustes cuando sea necesario.

Respecto a la seguridad de la cadena de suministro, las empresas que han implementado medidas para garantizar la visibilidad en su cadena están dando un paso importante hacia una mayor seguridad. Sin embargo, es necesario que todas las empresas tomen conciencia de la importancia de esta cuestión y adopten las medidas necesarias para proteger sus negocios.

Los datos de la encuesta muestran que la capacitación y concienciación de los empleados es una inversión clave para garantizar la

ciberseguridad de una organización. Las empresas deben continuar implementando y mejorando sus programas de capacitación para asegurar que sus empleados estén equipados para enfrentar los desafíos actuales y futuros.

Las empresas son cada vez más conscientes de la importancia de la ciberseguridad y están tomando medidas proactivas para proteger sus activos. La formación de los empleados, la protección de datos y un enfoque integral de la seguridad son los pilares fundamentales de estas estrategias. Sin embargo, es importante recordar que el panorama de las ciberamenazas es dinámico y en constante evolución. Por lo tanto, las empresas deben estar preparadas para adaptarse y adoptar nuevas tecnologías y medidas de seguridad a medida que surjan.


1
Evaluar los riesgos
Identificar vulnerabilidades y riesgos potenciales
2
Implementar controles
Reforzar la postura de seguridad
3
Documentar las políticas
Garantizar procedimientos y documentación adecuados
4
Formación del personal
Sensibilizar y desarrollar competencias en ciberseguridad
5
Revisiones regulares
Monitorización continua y adaptación a nuevas amenazas

Javier Carvajal: “La seguridad de la cadena de suministro es una de las diferencias que impone NIS2”

NIS2 es la Directiva Europea de Ciberseguridad más compleja que se ha formalizado. La normativa impone una serie de obligaciones a las empresas afectadas como la necesidad de que identifiquen, evalúen y gestionen los ciberriesgos a los que están expuestas.

Rosalía Arroyo

Javier Carvajal, CEO y socio fundador de **Icraitas**

Tomar el pulso al mercado, saber qué desafíos están afrontando las empresas españolas a la hora de hacer frente a la normativa o qué mecanismos están implementando para tener control sobre la cadena de suministro ha sido el objetivo de una encuesta realizada a más de cien empresas españolas de diferentes tamaños y sectores. La presentación y análisis de los resultados corrió a cargo deJavier Carvajal, CEO y socio fundador de Icraitas, y se realizó durante un encuentro

que reunió a casi una veintena de responsables de TI o ciberseguridad de empresas españolas, además de los cinco patrocinadores del mismo: Econocom, Fortinet, Mastercard, Pure Storage y Veeam.

Arrancaba su análisis Javier Carvajal refiriéndose a NIS2 como "la gran esperada" y, al mismo tiempo, "la gran desconocida", y recordando que la normativa, que sigue a NIS, deriva de lo que ocurrió en 2022, "cuando se produce una aproximación entre los dos grandes mundos normalizadores: el mundo americano y el mundo europeo". Fue en ese año cuando la ISO27001 se alinea con los postulados del *framework* NIST y, en España, el Real Decreto 311-2022, que es el ENS, el Esquema Nacional de Seguridad. Todas ellas pusieron de manifiesto que "hay una preocupación por la ciberseguridad".

Sobre el perfil de encuestados para el estudio destacaba Javier Carvajal que el 90 % han sido directivos, algo relevante "porque NIS2 pone el foco de responsabilidad directamente en la alta dirección".

Preguntado a los encuestados *"¿Qué pasos ha tomado para realizar una evaluación inicial del cumplimiento de NIS2 en su empresa?"*, destacaba Javier Carvajal que los datos revelan un avance significativo en la preparación de las empresas, con un enfoque en la revisión de políticas, la evaluación de planes de continuidad y la realización de análisis de riesgos. Sin embargo, aún persisten áreas donde se requiere mayor atención, concluía el CEO de Icraitas, quien, siguiendo con el análisis de las gráficas, comentaba que los principales desafíos para cumplir con la NIS2 están relacionados con la falta de compromiso de la alta dirección, la escasez de conocimientos técnicos y recursos financieros, y la complejidad de la normativa. Sin embargo, los resultados relacionados con la pregunta *"¿Cuáles son los prin-*

> "NIS2 pone el foco de responsabilidad directamente en la alta dirección"

> "Ya no vale la monitorización puntual porque los ciberdelincuentes están trabajando día y noche. Hay que ir hacia la monitorización continua"

cipales desafíos que enfrenta su empresa para cumplir con la Directiva NIS2?" también ponen de manifiesto que existe una creciente conciencia sobre la importancia de la ciberseguridad y que las empresas están tomando medidas para abordar estos desafíos.

Destacaba también Javier Carvajal la necesidad de un enfoque más integral y colaborativo para facilitar la implementación de NIS2 ya que, al combinar esfuerzos para simplificar la normativa, aumentar la financiación y proporcionar una mayor orientación, "se puede ayudar a las empresas a proteger sus sistemas y datos de manera más efectiva". En base a los datos recogidos en la pregunta *"¿Qué medidas cree que las autoridades podrían tomar para facilitar la implementación de la Directiva NIS2 por parte de las empresas?"*, el experto señalaba que las empresas enfrentan desafíos significativos al implementar la Directiva NIS2, a pesar de los esfuerzos de

las autoridades. Comentaba Javier Carvajal que, aunque existen iniciativas como el Kit Consulting, se necesita más financiación para apoyar a las empresas, especialmente a las pymes, en la implementación de las medidas de seguridad. Por otra parte, recordaba que la creciente cantidad de regulaciones en materia de ciberseguridad dificulta su comprensión y aplicación por parte de las empresas y concluía que, si bien las autoridades proporcionan cierta orientación, esta no siempre es accesible ni suficiente para cubrir las necesidades de las empresas.

Analizaba Javier Carvajal los resultados de *"¿Qué medidas ha tomado su empresa para aumentar su ciberseguridad y prepararse para NIS2 en el último año?"* destacando que la mayoría de las organizaciones ya han iniciado un proceso de mejora en su seguridad. Concluía que las empresas son cada vez más conscientes de la importancia de la ciberseguridad y están tomando medidas proactivas para protegerse; que NIS2 está actuando como un catalizador para impulsar la mejora de las medidas de seguridad

en las organizaciones; que las empresas están adoptando un enfoque integral de la ciberseguridad, que incluye tanto medidas técnicas como de concienciación y gestión de incidentes y que las organizaciones reconocen la importancia de mantener un proceso de mejora continua en materia de ciberseguridad para hacer frente a la evolución constante de las amenazas.

Garantizar la seguridad de la cadena de suministro es uno de los aspectos más destacados de la normativa. Frente a los resultados asociados a la pregunta *"¿Qué mecanismos ha implementado para garantizar una visibilidad completa y continua de la seguridad en toda su cadena de suministro?"* destacaba Javier Carvajal la importancia de la visibilidad y seguridad en la cadena de suministro, señalando que los mecanismos tradicionales, como los contratos, no son suficientes para prevenir incidentes. Enfatizaba la colaboración entre los diferentes actores de la cadena de suministro, especialmente con empresas más pequeñas que pueden carecer de los recursos necesarios y proponía la implementación de sistemas de monitorización continua para detectar amenazas, destacando al mismo tiempo la importancia de realizar evaluaciones de riesgo y auditorías periódicas.

> "No hay nadie en el mundo que no tenga una cadena de suministro"

Al analizar los resultados de la encuesta sobre *"¿Cómo asegura la capacitación y concienciación de los empleados sobre las obligaciones y medidas de seguridad bajo NIS2?"* reconocía Javier Carvajal que se han dado pasos importantes, pero consideraba que se podría haber avanzado más. Destacaba la importancia de la participación de la alta dirección en estos procesos, señalando que no solo los empleados, sino también los directores generales y consejeros, son responsables ante las consecuencias de cualquier incumplimiento. El experto

> “Los primeros que tienen que estar formados son los directivos, la alta dirección”

enfatizó que la formación no debe limitarse a los equipos técnicos, sino que debe extenderse a todos los niveles de la organización, especialmente a la alta dirección, subrayando que NIS2 impone la necesidad de que los directivos tengan una sensibilidad especial hacia los temas de ciberseguridad y que, si no la poseen, “hay que conseguir que la tengan”.

La última pregunta que se hacía a los encuestados tenía que ver con inversiones a futuro: “*¿En qué ámbitos planea focalizarse su empresa para aumentar su ciberseguridad en el próximo año?”.* En base a los resultados, destacó Javier Carvajal la importancia de varias áreas, como la formación de empleados y directivos, la mejora de las medidas de protección de datos, las auditorías de seguridad, el control de acceso, la implementación de sistemas de gestión de seguridad de la información y las medidas de recuperación ante desastres.

Durante su análisis dejó claro el CEO de Icraitas que las auditorías realizadas por terceros independientes son cruciales para identificar vulnerabilidades y garantizar la objetividad de los resultados; que las empresas deben prestar atención a la seguridad de sus proveedores y socios comerciales, ya que una brecha en la cadena de suministro puede comprometer la seguridad de toda la organización; que es esencial contar con planes de recuperación sólidos para garantizar la continuidad del negocio en caso de incidentes; que los marcos como el CCN pueden servir como guía para implementar medidas de seguridad efectivas y que la monitorización constante de los sistemas y redes es esencial para detectar y responder a amenazas de manera proactiva.

NIS2: un escudo de seguridad para la era digital

La Directiva NIS2 (Network and Information Systems) es una normativa de la Unión Europea diseñada para reforzar la ciberseguridad de los sectores esenciales y estratégicos. Su objetivo principal es garantizar un alto nivel común de ciberseguridad en toda la Unión Europea, ante el creciente número y sofisticación de los ciberataques.

Rosalía Arroyo

Reconociendo la creciente dependencia de las tecnologías de la información y la comunicación, NIS2 se centra en proteger sectores como la energía, el transporte, la salud, las finanzas y las telecomunicaciones, que son fundamentales para el funcionamiento de nuestras sociedades. En comparación con su predecesora, la NIS2 impone requisitos más estrictos y detallados en materia de ciberseguridad, obligando a las organizaciones a adoptar medidas más robustas.

La NIS2 se aplica a una amplia gama de organizaciones, que deben cumplir con una serie de obligaciones, entre las que destacan la necesidad de realizar una evaluación exhaustiva de sus ciberriesgos y establecer medidas de seguridad adecuadas, además de establecer procedimientos claros para la detección, notificación y respuesta a incidentes de ciberseguridad, o contar con planes para garantizar la continuidad de sus operaciones en caso de ciberataques. Las entidades afectadas deben colaborar con las autoridades competentes en materia de ciberseguridad y adoptar medidas para proteger la cadena de suministro de ciberataques.

Tomar el pulso al mercado, saber qué desafíos están afrontando las empresas españolas a la hora de hacer frente a la normativa o qué mecanismos están implementando para tener control sobre la cadena de suministro ha sido el objetivo de una encuesta realizada a más de cien empresas españolas de diferentes tamaños y sectores. Los resultados del Barómetro NIS2 se mostraron durante una presentación a la que asistieron diferentes responsables de TI y ciberseguridad de casi una veintena de empresas españolas, y portavoces de los patrocinadores, a los que después se invitó a participar en un debate.

Contamos con la presencia de Diego Durantes, CISO de AENOR; Manuel Moro, CIO/CISO de

Banco Caminos/CBNK; Jorge Crespo, director de operaciones TI de Capital Energy; Tamara Vicente, abogada sénior del departamento de ciberseguridad y privacidad de Écija Abogados; Francisco Sánchez, *IT security director* de Ecovadis; Pedro Navas, *manager sourcing & IT advisory* de Eraneos; José Manuel Rivera, *security officer* de Fintonic; Enrique Ferrer, CIO de Ford España; Vicente Camus, *cybersecurity manager* de Globalvia; Rafael Ceres, global ISO de Iberdrola; Jesús Valverde, CI/CISO de Isemaren; Luis Ángel Reinoso, director de ciberseguridad de Forbis Mazars; Daniel Damas, *head of assurance* de Nationale Nederlanden; David de la Rosa, CISO de Sanoma Educación SL; Alejandro Expósito, CIO/CISO/COO de Servatrix Biomédica; María del Pino González-Junco, ciberseguridad *partnerships manager* de Siemens; Pedro Fernández-Villamea, profesor universitario *legal&compliance* de la UAX; Javier Carvajal, CEO de Icraitas; Santiago Pérez, *territory cloud manager* de Veeam Software; Roberto Montero, director general de servicios de Econocom; Agustín Valencia, OT/ICS/xIoT *cyber security business development* de Fortinet; Alberto López, VP, *cyber & intelligence solutions product lead* Mastercard Europa;

> "Lo importante es demostrar que estamos trabajando de forma proactiva para cumplir con la normativa"
>
> **Manuel Moro,**
> CIO/CISO de **Banco Caminos/CBNK**

y Adela de Toledo, *country manager* Iberia de Pure Storage.

A **Pedro Navas** los resultados no le sorprenden. Comenta que es lógico que, dada la mayor conciencia sobre la ciberseguridad, haya un creciente interés en la NIS2, que las empresas están invirtiendo más en seguridad, "lo cual es positivo. Antes se veía como un gasto, ahora se reconoce como una inversión necesaria".

En opinión de **Jesús Valverde**, NIS2 ha evidenciado que muchos de los contratos firmados por las empresas pueden estar obsoletos y ser poco prácticos. "¿Cuántos de nosotros seguimos negociando contratos de encargado de tratamiento que dejan en el aire la responsabilidad de gestionar los riesgos?", plateaba el directivo durante el encuentro, añadiendo una cuestión: "¿Cuántos de vosotros habéis recibido alguna propuesta de modificación de un contrato de una entidad afectada por NIS2 a la que prestéis servicio para agregar o evidenciar algún tipo de medida de seguridad adicional a lo que ya estuvieseis haciendo antes?".

Destacaba **David de la Rosa** que los datos presentados son muy interesantes y revelan un patrón curioso: aproximadamente un 20 % de las empresas muestran una clara relación entre la falta de apoyo de la dirección y el desconocimiento sobre la aplicación de la normativa. "Esta coincidencia es significativa, ya que sugiere que cuando los directivos no comprenden plenamente los requisitos legales, es menos probable que brinden el apoyo necesario para las mejoras de seguridad que estos marcos normativos impulsan", aseguraba el directivo de Sanoma Educación.

Comentado que llevan tiempo trabajando en DORA, resaltaba **Luis Reinoso, director de ciberseguridad de Forvis Mazars**, haberse sentido sorprendido por el desconocimiento sobre

"Una de las mayores preocupaciones al implementar la NIS2 es la armonización con otras regulaciones internacionales"

María del Pino González-Junco,
ciberseguridad partnerships manager de **Siemens**

la normativa. Recordaba que en el mercado hemos sido testigos de cómo, con normativas similares como la GDPR, "incluso a pocos días de su entrada en vigor, las autoridades aún no tenían claras las directrices. Ahora, con un alcance mucho mayor y un impacto en sectores tan diversos como la alimentación, la situación es aún más alarmante".

"Los datos son preocupantes, aunque no sorprendentes", aseguraba **Daniel Damas, *head of assurance* de Nationale Nederlanden**, añadiendo que la comunicación por parte del regulador podría haber sido confusa y generado cierta incertidumbre. Poniéndose manos a la obra, el directivo utilizó herramientas de inteligencia artificial para que la directiva comprendiera mejor sus responsabilidades; "muchos se mostraron preocupados al descubrir las posibles consecuencias penales en caso de incumplimiento".

Planteado durante el debate qué es lo que más preocupa de la directiva, comentaba **Francisco Sánchez, *IT security director Spain* de Ecovadis**, que la transposición de la NIS2 a nivel nacional es un gran desafío para las empresas con presencia en múltiples países. Que cada estado miembro pueda introducir sus propias interpretaciones y requisitos adicionales, "genera una gran complejidad a la hora de garantizar el cumplimiento normativo", comentaba el directivo.

"La falta de definiciones claras sobre cómo implementar nuestras medidas de seguridad genera una gran incertidumbre"

Enrique Ferrer,
CIO de **Ford España**

Retos de NIS2 - ¿Qué preocupa?

"Una de las mayores preocupaciones al implementar la NIS2 es la armonización con otras regulaciones internacionales", comentaba **María del Pino González-Junco, ciberseguridad**

> "La nueva normativa exige notificar las incidencias en 24 horas, lo que crea un dilema con nuestros proveedores, especialmente los más pequeños, que podrían no ser capaces de cumplir con este plazo"

Daniel Damas Díaz,
head of assurance de **Nationale Nederlanden**

***partnerships manager* de Siemens**. Explicaba que las empresas que operan a nivel global se enfrentan al desafío de conciliar los requisitos de la NIS2 con los de otros países, como Estados Unidos y que, para abordarlo, se han creado grupos de trabajo dedicados a monitorizar y analizar la transposición de la directiva en cada país, "con el objetivo de identificar las mejores prácticas y anticiparnos a los cambios regulatorios".

Por otra parte, "la cadena de suministro representa una complejidad adicional en la implementación de NIS2", aseguraba la responsable de Siemens mencionando que la gran variedad de proveedores y la diversidad de sus roles hacen que sea difícil establecer procedimientos únicos para todos, por lo que se ha adoptado "un enfoque basado en la clasificación de riesgos, priorizando aquellos proveedores que podrían tener un mayor impacto en nuestra seguridad".

En el caso de **Vicente Camus, *cybersecurity manager* de Globalvia**, la experiencia de la compañía operando a nivel internacional y las medidas de ciberseguridad que ya tienen implementadas, hacen que "la adopción de la NIS2 no represente un desafío significativo para nuestra organización. De hecho, muchos de los requisitos de la NIS2 están alineados con las

> "Es importante recordar que la seguridad es un viaje, no un destino"

Santiago Pérez,
territory cloud manager de **Veeam Software**

prácticas que ya hemos establecido", decía el directivo, reconociendo que "siempre hay áreas de mejora, como la profundización en el análisis de riesgos. No obstante, consideramos que estamos bien preparados para cumplir con los requisitos de la NIS2, y que la implementación de esta normativa no requerirá un esfuerzo adicional considerable".

"Es esencial contar con herramientas que permitan recuperar los datos de forma ágil y segura"

Adela de Toledo,
country manager Iberia de **Pure Storage**

Intervenía **Roberto Montero, director general de servicios de Econocom**, para comentar que, cuando se trata de normativas, "la comprensión de la dirección es fundamental" y que, en muchas ocasiones, "son las multas las que mueven presupuestos".

"La asignación de responsabilidades es fundamental para el éxito de cualquier iniciativa de seguridad", aseguraba **Santiago Pérez, *territory cloud manager* de Veeam Software**, añadiendo que, aunque cumplir con normativas como la NIS2 y la DORA puede parecer abrumador al principio, "ofrece una ventaja: al abordar los requisitos más estrictos, se establecen las bases para una seguridad sólida. Es importante recordar que la seguridad es un viaje, no un destino. Debemos trabajar continuamente para mejorar nuestros sistemas y procesos".

"La ciberseguridad no es solo un requisito legal, es una necesidad empresarial", recordaba **Alberto López, *VP, cyber & intelligence solutions product lead* de Mastercard** Europa, comentando que la pérdida de datos, la interrupción de los servicios y el daño a la reputación pueden tener un impacto devastador en cualquier organización. Aseguraba sentirse sorprendido de que, "con una directiva como NIS2, que está aprobada, aunque no está transpuesta, haya un 30 % de empresas que, o bien no sabe si le afecta, o ni siquiera ha empezado a analizar nada al respecto. Uno de cada tres es una cifra que no sé si decir que sorprende, pero

"La ciberseguridad no es solo un requisito legal, es una necesidad empresarial"

López González, *VP, cyber & intelligence solutions product lead* de **Mastercard Europa**

al menos asusta, porque no hace falta tener la transposición para empezar a trabajar ya".

Destacaba durante su intervención **Adela de Toledo, *country manager* Iberia de Pure Storage**, que es interesante ver cómo las empresas están destinando una gran parte de su presupuesto a la innovación en seguridad cibernéti-

ca, pero que este panorama tan fragmentado, con múltiples proveedores y soluciones, "genera una complejidad que dificulta la toma de decisiones". En opinión de la directiva, "lo más importante es enfocarse en restaurar la confianza lo más rápido posible después de un incidente de seguridad", para lo cual "es esencial contar con herramientas que permitan recuperar los datos de forma ágil y segura. La clave está en seleccionar las soluciones más adecuadas y fáciles de implementar, priorizando aquellas que nos permitan responder de manera efectiva ante una amenaza", aseguraba.

NIS2 nos presenta un gran desafío: priorizar entre tantas medidas de seguridad, dice **Agustín Valencia, OT/ICS/xIoT *cyber security business development* de Fortinet**, explicando que las pequeñas empresas se centran en lo básico, como la protección perimetral y el correo electrónico, mientras que las grandes empresas y las infraestructuras críticas consideran impactos más profundos. Experto en entornos OT, aseguraba el directivo de Fortinet que, en entornos industriales, la gestión de vulnerabilidades es especialmente compleja y que, al evaluar el

riesgo de los activos, debemos considerar no solo su valor intrínseco, sino también su impacto en los ingresos de la empresa".

Retos de NIS2 - Cadena de suministro

Las organizaciones modernas están cada vez más interconectadas, con múltiples proveedores y socios comerciales. La Directiva NIS2 ha puesto un énfasis particular en la seguridad de la cadena de suministro, un enfoque que reconoce que las vulnerabilidades en los proveedores y socios comerciales pueden comprometer la seguridad de toda la organización.

Decía **Rafael Ceres, global CISO de Iberdrola**, que NIS2 obliga a ser estratégicos en la gestión de la ciberseguridad. "Debemos pasar de un enfoque basado en controles a uno centrado en los riesgos", lo que implica identificar los riesgos más críticos y priorizar las acciones en consecuencia. La gestión de terceros es un ex-

"Prefiero ver NIS2 como una oportunidad para fortalecer nuestra cultura de seguridad, más allá de un mero cumplimiento normativo"

Rafael Ceres Campos,
global CISO de **Iberdrola**

celente ejemplo de cómo una mala priorización "puede llevarnos al fracaso".

Dejaba claro durante su intervención **Manuel Moro, directivo de Banco Caminos/CBNK**, que el mayor desafío que afronta como entidad financiera "no es tanto la gestión de riesgos internos, como la notificación de incidentes a clientes", además de la gestión del riesgo "de nuestra cadena de suministro, especialmente al trabajar con pymes". Explicaba que a menudo las auditorías excesivas pueden ser perjudiciales para estas empresas más pequeñas y que, aunque necesarios, los ciberseguros no pueden compensar completamente la pérdida de reputación tras una brecha de seguridad. "En resumen, nuestra superficie de ataque se extiende más allá de nuestras propias fronteras y gestionar este riesgo externo es fundamental".

Planteaba **Enrique Ferrer, CIO de Ford**, que NIS2 presenta desafíos únicos para el sector automotriz. "Mientras que nuestros proveedores principales suelen cumplir con altos estándares de seguridad, nuestra red de concesionarios presenta una mayor diversidad en términos de tamaño y capacidades", aseguraba. Resaltaba que, a diferencia de otros sectores, la mayoría de los ciberataques que se dirigen contra su compañía buscan la propiedad intelectual, más que datos personales; "esto significa que nuestras prioridades en materia de seguridad pueden diferir de las de otras industrias". La aplicación de la NIS2 a nivel global también plantea interrogantes sobre la proporcionalidad de las medidas de seguridad en diferentes mercados, comentaba Ferrer.

"Es importante recordar que la ciberseguridad es un proceso continuo y que la normativa evoluciona constantemente"

Tamara Vicente Rodríguez,
abogada sénior del departamento de ciberseguridad y privacidad de **Écija Abogados**

"Es fundamental tener procesos bien definidos y ensayados para la notificación de incidentes"

David de la Rosa,
CISO de **Sanoma Educación SL**

En calidad de abogada sénior del departamento de ciberseguridad y privacidad de Écija Abogados, **Tamara Vicente** comentaba que las negociaciones con proveedores, especialmente las pymes, son complejas. Si bien puede darse el caso de que se priorice la firma de un contrato por encima del cumplimiento de los estándares de seguridad, también se observa una resistencia en las grandes empresas a asumir responsabilidades amplias. "Esto nos plantea un dilema: ¿aceptamos condiciones menos favorables para mantener a un proveedor crítico o buscamos alternativas a un mayor costo?", resaltaba Tamara Vicente asegurando que la cadena de suministro representa un riesgo significativo "debido a estas dificultades en la negociación y colaboración en materia de seguridad."

Retos de NIS2 – Notificación de incidentes

"La notificación de incidentes según la NIS2 representa un nuevo desafío", comentaba **José Manuel Rivera, *security officer* de Fintonic**, donde se apuesta por promover una cultura de seguridad en toda la organización, fomentando la colaboración entre todos los equipos. En segundo lugar, "estamos desarrollando herramientas y procesos para evaluar de manera cuantitativa el impacto de los incidentes y determinar cuándo es necesario notificarlos a las autoridades". Por último, "estamos capacitando a nuestros empleados, especialmente a los gerentes, para que puedan identificar y reportar incidentes de manera oportuna".

"¿Cuántos habéis recibido alguna propuesta de modificación de un contrato de una entidad afectada por NIS2?"

Jesús Valverde Romero,
CI/CISO de **Isemaren**

Aunque pueda parecer sencillo, el proceso de notificación de una brecha de seguridad es mucho más complejo de lo que parece. Así lo aseguraba **David de la Rosa, CISO de Sanoma Edu-**

"Las pymes no suelen contar con los medios necesarios para cumplir con las nuevas regulaciones"

Diego Durantes, CISO de **AENOR**

cación SL, quien aseguraba que, bajo presión y con un tiempo limitado, "es fácil olvidar información crucial". Por eso, añadía, "es fundamental tener procesos bien definidos y ensayados, que involucren a todos los niveles de la organización, desde la dirección hasta los equipos técnicos".

Explicaba **Jesús Valverde, CI/CISO de Isemaren** que el protocolo de notificación de la compañía "establece claramente los pasos a seguir en caso de incidentes de seguridad, especialmente aquellos que comprometen datos personales". No obstante, cuando se trata de entornos OT, "la responsabilidad de la detección y evaluación inicial recae en nuestros clientes", decía, añadiendo que, para garantizar una respuesta efectiva, "trabajamos en estrecha colaboración con ellos, definiendo los canales de comunicación y estableciendo un marco de colaboración que permita identificar y abordar rápidamente cualquier incidente".

La cadena de suministro es un eslabón débil en la ciberseguridad. Comentaba **Agustín Valencia, directivo de Fortinet**, que a menudo los contratos son insuficientes para garantizar la seguridad de los proveedores y que cada vez son más necesarias "las herramientas que permitan identificar rápidamente las vulnerabilidades en toda la cadena de suministro, como filtraciones de credenciales". Añadía que normativas como DORA y NIS2 proporcionan un marco para abordar estos desafíos, pero que

"Los contratos son insuficientes para garantizar la seguridad de los proveedores"

Agustín Valencia, OT/ICS/xIoT *cyber security business development* de **Fortinet**

"la falta de interoperabilidad entre las regulaciones globales sigue siendo un obstáculo". Debemos trabajar hacia una mayor armonización de los requisitos técnicos para reducir la carga administrativa y mejorar la eficiencia, aseguraba también Agustín Valencia.

"En situaciones de crisis, la comunicación clara

y efectiva es fundamental", aseguraba **Adela de Toledo**, añadiendo que se hace necesaria una estrategia de comunicación interna bien definida "que nos permita transmitir información precisa y oportuna a todos los involucrados. Esta estrategia debe ser sencilla y fácil de entender para evitar confusiones y garantizar una respuesta coordinada".

La cadena de suministro es un vector de ataque cada vez más común, recordaba **Alberto López, directivo de Mastercard**. Añadía que, para mitigar este riesgo, "es esencial contar con herramientas que nos permitan evaluar la ciberseguridad de nuestros proveedores de manera continua" y que no basta con una auditoría inicial, sino que "debemos realizar evaluaciones periódicas para asegurarnos de que siguen cumpliendo con nuestros estándares". Dejaba claro durante su intervención que NIS2 obliga a ser más proactivos en la gestión de estos riesgos, que se debe ir más allá de los requisitos contractuales "y realizar una *due diligence* técnica de nuestros proveedores. Si un proveedor no demuestra un compromiso sólido con la ciberseguridad, representa un riesgo inaceptable para nuestra organización".

Las pequeñas empresas son especialmente vulnerables a los ciberataques, y son parte de la cadena de suministro de las grandes. En opinión de **Santiago Pérez, directivo de Veeam**, "determinar el nivel de seguridad adecuado es un desafío, pero la notificación de incidentes es un primer paso fundamental".

Contó el caso de cómo el gobierno de Estados Unidos detectó, infiltrándose en un grupo de ciberdelincuentes, no sólo cuánto ganaban, sino qué empresas habían tenido una brecha de seguridad y no habían informado de ello, "quien no notificaba". Aseguró durante su intervención **Santiago Pérez** que, al comprender las tácticas de los atacantes, podemos implementar medidas preventivas más efectivas. Además, la rápida notificación de incidentes permite una res-

"Los terceros juegan un papel crucial en nuestras operaciones diarias, y su gestión es un desafío constante"

Roberto Montero,
director general de servicios de **Econocom**

puesta más coordinada y reduce el impacto de los ataques.

Dejaba claro **Roberto Montero, de Econocom**, que los terceros "juegan un papel crucial en nuestras operaciones diarias, y su gestión es un desafío constante". Para minimizar los riesgos asociados a la cadena de suministro, "es imprescindible que todos los actores involucrados, desde los proveedores hasta los socios tecnológicos, tengan un conocimiento profundo del negocio de sus clientes", decía también, añadiendo que, al trabajar en conjunto y compartir información de manera transparente, "podemos identificar y mitigar las vulnerabilidades antes de que se conviertan en problemas mayores. De lo contrario, un solo incidente puede tener un impacto devastador en la reputación de toda la cadena".

Retos de NIS2 – Respuesta ante incidentes

Recordaba **Daniel Damas, de Nationale Nederlanden**, que la nueva normativa exige notificar las incidencias en 24 horas, lo que "crea un dilema con nuestros proveedores, especialmente los más pequeños, que podrían no ser capaces de cumplir con este plazo". Añadía el directivo que, "si no podemos garantizar que nuestros proveedores nos notifiquen a tiempo, corremos el riesgo de incumplir la ley. Esta situación dificulta la contratación de nuevos proveedores y pone en riesgo nuestra capacidad de cumplir con la normativa".

"Mientras esperamos la transposición de la directiva, debemos actuar de forma proactiva"

Pedro Fernández-Villamea, profesor universitario *legal&compliance* de la **UAX**

Resaltaba **Jorge Crespo, director de operaciones TI de Capital Energy**, la importancia de tener canales de comunicación internos eficientes y que, con el fin de mejorar, la compañía ha implementado nuevos procesos "que nos permiten identificar y responder a los incidentes

"La falta de claridad normativa genera dudas sobre cómo actuar"

Luis Ángel Reinoso Tello,
director de ciberseguridad de **Forvis Mazars**

de manera más rápida y efectiva". Además, se ha involucrado a los equipos de dirección en la toma de decisiones, "lo que agiliza la resolución de problemas", lo que llevó al directivo a señalar que se busca "garantizar que nuestros procesos cumplan con los más altos estándares de seguridad".

Se plantea durante el debate que, para cumplir con NIS2, hay que comunicar un incidente en 24 horas, pero que, si un proveedor no dice nada ¿qué vas a reportar?

Introducía **Pedro Fernández-Villamea, profesor universitario de *legal y compliance* de la UAX**, el concepto *culpa in vigilando* asegurando que "mientras esperamos la transposición de la directiva, debemos actuar de forma proactiva" y que, aunque no tengamos una normativa completamente definida, "podemos establecer ciertas obligaciones de seguimiento hacia nuestros proveedores". Explicaba que, dependiendo de las normativas, existen diferentes plazos para comunicar una brecha (24h para NIS, 72h para RGPD), "pero la esencia es la misma: debemos exigir a nuestros proveedores que nos mantengan informados. De esta manera, demostramos nuestra buena fe y nos protegemos ante posibles incumplimientos".

Mencionaba Pedro Fernández-Villamea que se debe analizar la situación desde cuatro perspectivas: riesgos, retos, responsables y responsabilidades para señalar que a menudo confundimos riesgo con amenaza, pero que mientras el riesgo es interno y controlable, la amenaza viene del exterior. Aseguraba que "el reto principal es adelantarnos a las normativas, no esperar a que nos indiquen cada paso", y que las empresas que actúan de manera proactiva obtienen una ventaja competitiva.

"Es esencial no perder de vista el objetivo principal de la directiva NIS2: prevenir ciberataques y proteger los sistemas críticos"

Javier Carvajal,
CEO de **Icraitas**

"La incertidumbre generada por las transposiciones nacionales dificulta nuestra capacidad para transmitir confianza a la dirección"

Francisco Sánchez Nauffal,
IT security director de **Ecovadis**

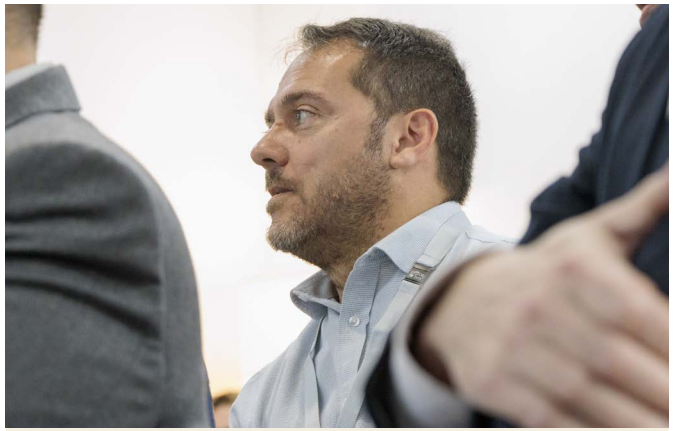
En cuanto a responsabilidades, "debemos fomentar una cultura de cumplimiento, basada en la convicción y no solo en el miedo a las sanciones", decía el profesor, añadiendo que la formación continua es fundamental, "pero a menudo nos quedamos en la teoría sin pasar a la práctica".

Intervenía **Javier Carvajal** para mencionar que "es esencial no perder de vista el objetivo principal de la directiva NIS2: prevenir ciberataques y proteger los sistemas críticos", y que "aunque la diligencia debida puede ser una herramienta útil, no exime de la responsabilidad de cumplir con los requisitos de la directiva. Esta entró en vigor hace ya un tiempo y su aplicación no depende exclusivamente de la finalización de los procesos de transposición nacionales".

Impacto de la no transposición

El 17 de octubre de 2024 se alcanzó la fecha límite para la transposición en los Estados miembros de la Directiva NIS2. ¿Qué impacto tiene esa no transposición?

Para **Jesús Valverde,** la falta de transposición de la NIS2 en España dificulta la implementación de medidas de ciberseguridad homogéneas en el sector energético. "Empresas como Isemaren, que operan en este sector, se encuentran en una situación compleja. Por un lado, nuestros clientes cada vez demandan mayores garantías de seguridad, pero por otro, la ausencia de una normativa clara nos impide establecer un plan de cumplimiento uniforme a nivel de grupo", explica el CIO/CISO de la compañía, asegurando además que es fundamental



"El plan de seguridad actual de la compañía será suficiente, quizá con pequeños cambios, cuando llegue la transposición"

Jorge Crespo,
director de operaciones TI de **Capital Energy**

garantizar un mayor nivel de protección para las infraestructuras críticas.

La falta de claridad normativa dificulta la toma de decisiones estratégicas en materia de ciberseguridad. Así de claro se mostraba **José Manuel Rivera, *security officer* de Fintonic**, explicando que la constante evolución del panorama normativo "nos obliga a reevaluar constantemente nuestras prioridades y a destinar recursos a áreas que pueden cambiar rápidamente". Esta incertidumbre dificulta la creación de una estrategia de ciberseguridad a largo plazo.

En opinión de **David de la Rosa**, la falta de claridad normativa frena la innovación y reduce la competitividad; "sin directrices claras, es imposible desarrollar productos y servicios que cumplan con todos los requisitos de seguridad. Además, recuerda que esta situación también afecta a la Administración pública que, "al no contar con un marco normativo definido, exigirá a los proveedores respuestas cada vez más rápidas, a las que no podremos atender de manera eficiente".

Sumándose a las opiniones expresadas aseguraba **Luis Ángel Reinoso, director de ciberseguridad de Forvis Mazars**, que "la falta de claridad normativa genera dudas sobre cómo actuar" y que ante la situación se opta por ser proactivos y adoptar el ENS, que si bien no es un requisito legal en todos los países donde operamos, "es una medida preventiva necesaria". Al ser una firma de servicios profesionales, "manejamos información sensible y debemos cumplir con las regulaciones más exigentes en materia de protección de datos".

Compartiendo la preocupación sobre que la falta de claridad por la no transposición afecte a que se garantice que se estén adoptando las medidas correctas, aseguraba **Vicente Camus, *cybersecurity manager* de Globalvia**, que la asignación de recursos es una decisión crucial "y debemos asegurarnos de tomarla de manera informada".

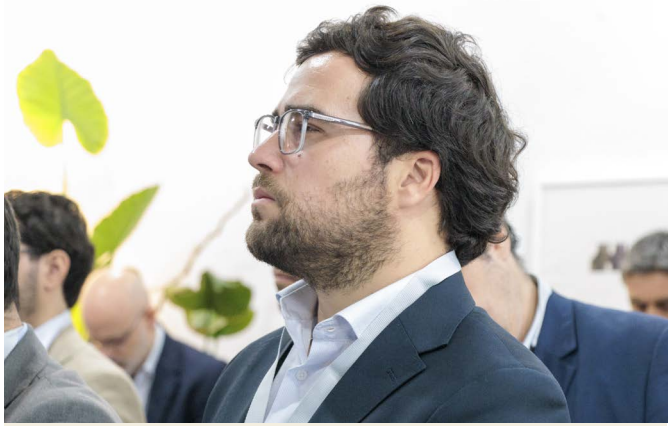
> "La cadena de suministro y los proveedores son puntos críticos que requieren una atención especial"
>
> **Pedro Navas,** *manager sourcing & IT advisory* de **Eraneos**

Para **María del Pino González-Junco, ciberseguridad *partnerships manager* de Siemens**, "es crucial que la dirección comprenda que la incertidumbre sobre la transposición no debe paralizarnos. Debemos avanzar con una planificación proactiva, asumiendo que la NIS2 se aplicará pronto". Añadía que, si se posponen las acciones de adecuación, "nos arriesgamos a encontrarnos con una carga de trabajo excesiva cuando la normativa entre en vigor", por lo que es importante solicitar los recursos necesarios para iniciar las actividades de cumplimiento, "incluso considerando que podrían requerir ajustes en el futuro".

"El principal inconveniente es que un caso de negocio, por sólido que sea, se vuelve inestable si no cuenta con un marco legal sólido que lo respalde. Sin una ley clara, las proyecciones se vuelven especulativas y el resultado final es incierto", aseguraba **Daniel Damas Díaz, *head of assurance* de Nationale Nederlanden.**

Bromeaba **Jorge Crespo, director de operaciones TI de Capital Energy**, con incluir una línea extra en su presupuesto "por si acaso necesitamos hacer ajustes importantes" para después asegurar que el plan de seguridad actual de la compañía será suficiente, quizá con pequeños cambios, cuando llegue la transposición.

Dejaba claro **Francisco Sánchez, *IT security director* Spain de Ecovadis** que la incertidumbre generada por las transposiciones nacionales "dificulta nuestra capacidad para transmitir confianza a la dirección". Explicaba que, cuando nos piden que garanticemos el cumplimiento de regulaciones en constante evolución, es complicado ofrecer respuestas definitivas, y que, "si bien tenemos los aspectos generales cubiertos,



> "La implementación de NIS2 no requerirá un esfuerzo adicional considerable en Globalvia"
>
> **Vicente Camus,**
> *cybersecurity manager* de **Globalvia**

los detalles específicos de cada transposición pueden introducir nuevos desafíos".

Apostando por un mensaje optimista, decía **Rafael Ceres, global CISO de Iberdrola** que prefiere ver NIS2 como "una oportunidad para fortalecer nuestra cultura de seguridad, más allá de un mero cumplimiento normativo". Asegurando que la compañía tiene una comprensión clara de los ciberriesgos y de las medidas necesarias para mitigarlos, comentaba que, si bien la transposición "aún no está finalizada, podemos comenzar a implementar muchas de estas medidas desde ya. Estoy convencido de que, con un enfoque basado en el riesgo y en la mejora continua, lograremos un alto nivel de protección".

Respecto a la no transposición de la normativa, percibe **Pedro Fernández-Villamea, profesor universitario de la UAX**, dos riesgos: riesgo nación y riesgo poder. Sobre el primero aseguraba que, a pesar de que el Departamento de Seguridad Nacional ha identificado la ciberamenaza como la segunda mayor amenaza para nuestro país, "no vemos una prioridad similar en el Congreso a la hora de transponer directivas como la NIS2". Esta discrepancia "genera una incertidumbre significativa y afecta negativamente a la reputación de España a nivel internacional". En cuanto al riesgo poder, aseguraba que se debe garantizar la seguridad de nuestros proyectos, incluso en un entorno regulatorio incierto. "Si no proporcionamos soluciones de seguridad, nuestros proyectos se vuelven menos atractivos y corren el riesgo de fracasar", decía Fernández-Villamea.

"La notificación de incidentes según la NIS2 representa un nuevo desafío"

José Manuel Rivera García, *security officer* de **Fintonic**

En opinión de **Pedro Navas**, aunque no se tenga una visión completa, los datos disponibles son suficientes para tomar medidas. Comentaba que aquellas empresas que han invertido en seguridad ya cuentan con una base sólida, pero que "todas debemos seguir aprendiendo y adaptándonos a las nuevas amenazas. La cadena de suministro y los proveedores son puntos críticos que requieren una atención especial".

Dejaba claro **Enrique Ferrer** que la falta de definiciones claras sobre cómo implementar nuestras medidas de seguridad genera una gran incertidumbre. Es como intentar seguir un mapa que cambia constantemente: no sólo retrasa los avances, "sino que también aumenta el riesgo de errores".

Recordaba **Tamara Vicente Rodríguez, abogada sénior del departamento de ciberseguridad y privacidad de Écija Abogados**, que aunque el marco regulatorio aún esté en construcción, "la directiva europea nos proporciona una guía clara sobre los principios básicos de

ciberseguridad que debemos aplicar". Recordaba que la gestión de riesgos se vuelve fundamental, que se deben identificar "los riesgos más críticos para nuestra organización, implementando las medidas de seguridad necesarias para mitigarlos y estar preparados para adaptarnos a los cambios normativos futuros". Añadía al término de su intervención que es importante recordar que la ciberseguridad es un proceso continuo, y que la normativa evoluciona constantemente, "por lo que se debe adoptar una cultura de mejora continua".

"Coincido en que la situación de las grandes empresas, como las del IBEX 35, es preocupante la no transposición", decía **Diego Durantes, CISO de AENOR**, asegurando que le preocupa aún más la situación de las pequeñas y medianas empresas, que "suelen tener menos recursos y conocimientos sobre ciberseguridad, lo que las hace más vulnerables a los ataques". Finalizaba su intervención recordando que muchas pymes están enfocadas en el día a día de sus negocios "y no cuentan con los medios necesarios para cumplir con las nuevas regulaciones".

Frente a la no transposición de la normativa, propone **Manuel Moro, CIO/CISO de Banco Caminos/CBNK**, realizar un *Gap Analysis* que ayude a identificar los aspectos en los que una organización está más avanzada y aquellos en los que se debe mejorar; "al tener una visión clara de nuestra situación actual, podremos adaptarnos más fácilmente a los requisitos finales de la NIS2". Para el directivo, "lo importante es demostrar que estamos trabajando de forma proactiva para cumplir con la normativa. Si bien es cierto que aún no tenemos todas las respuestas, el hecho de haber iniciado este proceso y de haber identificado nuestras áreas de mejora será valorado positivamente".

“Somos responsables de la transformación digital de nuestros clientes”

Roberto Montero,
director general de servicios de **Econocom**

Somos una empresa de servicios que opera 24/7 y dependemos en gran medida de terceros proveedores para ofrecer nuestros servicios. Nuestra amplia gama de servicios, que incluye desde infraestructura hasta soluciones de trabajo colaborativo, nos expone a un mayor riesgo de ciberseguridad.

Por un lado, somos integradores de soluciones y llevamos a cabo proyectos a medida. Por otro, somos responsables de la transformación digital de nuestros clientes, lo que implica trabajar estrechamente con terceros. En ambos casos, la seguridad es un pilar fundamental.

> “Consideramos que es fundamental que todos los actores involucrados en nuestros servicios estén comprometidos con la seguridad de la información”

En nuestra organización, contamos con un equipo dedicado a la seguridad de la información que trabaja en estrecha colaboración con nuestros empleados y proveedores. Nuestras prioridades incluyen capacitar a nuestros empleados y a los de nuestros clientes sobre las mejores prácticas en seguridad cibernética; identificar y mitigar los riesgos de seguridad en nuestros sistemas y procesos; y trabajar estrechamente con nuestros proveedores para garantizar que cumplan con los más altos estándares de seguridad.

Consideramos que es fundamental que todos los actores involucrados en nuestros servicios, desde nuestros empleados hasta nuestros proveedores, estén comprometidos con la seguridad de la información. Solo así podremos garantizar la continuidad de nuestro negocio y proteger los datos de nuestros clientes.

“En el contexto de NIS2, Fortinet se posiciona como un socio estratégico”

Agustín Valencia,
OT/ICS/xIoT cyber security business development de **Fortinet**

Fortinet ofrece una plataforma integral de ciberseguridad que permite a las organizaciones consolidar sus soluciones de seguridad en una única plataforma. Esta plataforma no solo integra firewalls y antivirus, sino que también abarca áreas como la gestión de redes (SD-WAN), la detección de amenazas y la respuesta a incidentes.

La propuesta de valor de Fortinet se centra en simplificar la gestión de la seguridad, reducir la complejidad y mejorar la eficiencia. Al integrar múltiples soluciones en una sola plataforma, las organizaciones pueden optimizar sus recursos y responder de manera más efectiva a las amenazas cibernéticas.

> “La propuesta de valor de Fortinet se centra en simplificar la gestión de la seguridad, reducir la complejidad y mejorar la eficiencia”

Además, Fortinet destaca la importancia de la resiliencia y la continuidad del negocio. La empresa ofrece soluciones para gestionar de manera eficiente las comunicaciones, incluyendo la integración de diversas redes y la implementación de planes de continuidad del negocio.

En el contexto de la normativa NIS2, Fortinet se posiciona como un socio estratégico para ayudar a las organizaciones a cumplir con los requisitos de seguridad. La plataforma de Fortinet permite orquestar las capacidades de seguridad existentes y agregar nuevas funcionalidades, como la detección temprana de amenazas, para mejorar la protección de los sistemas y datos.

“Mastercard busca ayudar a las empresas a reducir sus riesgos y proteger sus operaciones”

Alberto López González,
VP, cyber & intelligence solutions product lead de **Mastercard Europa**

Mastercard, tradicionalmente conocida por su liderazgo en la industria de pagos, ha ampliado significativamente su alcance en el ámbito de la ciberseguridad. Con inversiones de miles de millones de dólares, la compañía ha desarrollado una suite completa de soluciones de seguridad que van más allá de la protección de transacciones.

> “Con inversiones de miles de millones de dólares, Mastercard ha desarrollado una suite completa de soluciones de seguridad”

Actualmente, Mastercard ofrece servicios de consultoría para ayudar a las empresas a entender y cumplir con las cada vez más complejas regulaciones en materia de ciberseguridad. Además, ha desarrollado una serie de herramientas basadas en inteligencia artificial que permiten simular ciberataques, evaluar la postura de seguridad de los proveedores y detectar vulnerabilidades en los sistemas de las organizaciones.

Al proporcionar una visión holística de la seguridad, Mastercard busca ayudar a las empresas a reducir sus riesgos y proteger sus operaciones. La compañía ha demostrado su compromiso con la ciberseguridad al invertir en tecnología de vanguardia y al adquirir empresas especializadas en diferentes áreas de seguridad.

“Nuestra propuesta se centra en ofrecer una solución robusta y eficiente para cumplir con NIS2”

Adela de Toledo,
country manager Iberia de **Pure Storage**

Nuestra propuesta se centra en ofrecer una solución robusta y eficiente para cumplir con los requisitos de la normativa NIS2. Al enfrentar la complejidad de esta regulación y la necesidad de garantizar la recuperación rápida de datos, hemos desarrollado una tecnología de almacenamiento inmutable que simplifica el proceso y minimiza los riesgos.

> “Basada en principios de simplicidad, nuestra solución permite almacenar los datos de manera segura y accesible, tanto en entornos locales como en la nube”

Nuestra solución, basada en principios de simplicidad, permite almacenar los datos de manera segura y accesible, tanto en entornos locales como en la nube. La inmutabilidad de los datos garantiza su integridad y evita la pérdida de información en caso de incidentes de seguridad. Además, nuestra tecnología ofrece una capacidad de recuperación excepcional, permitiendo restaurar grandes volúmenes de datos en cuestión de horas.

Al trabajar con clientes como ServiceNow, que presta servicios a grandes instituciones financieras, hemos demostrado la eficacia de nuestra solución en entornos altamente regulados. Nuestra experiencia nos permite ofrecer a nuestros clientes una propuesta sólida y adaptada a sus necesidades específicas.

“Es fundamental que todos los componentes de una infraestructura trabajen de manera coordinada”

Santiago Pérez,
territory cloud manager de **Veeam Software**

Como fabricantes, hemos aprendido que los ciberataques pueden ocurrir en cualquier momento y sin previo aviso. Por eso, la monitorización constante es esencial, incluso en nuestros propios sistemas de protección de datos.

A menudo detectamos los ataques de ransomware en las copias de seguridad, lo que demuestra la importancia de contar con repositorios inmutables. Sin embargo, muchas organizaciones no aprovechan al máximo estas herramientas al no tener activadas las alertas tempranas.

> “A menudo detectamos los ataques de ransomware en las copias de seguridad, lo que demuestra la importancia de contar con repositorios inmutables”

Creemos que es fundamental que todos los componentes de una infraestructura trabajen de manera coordinada. Esto implica una comunicación fluida entre los diferentes equipos y sistemas, y la integración de herramientas de seguridad como SIEM.

Además, es crucial probar regularmente los planes de recuperación ante desastres. La automatización de estos procesos es clave para responder de manera rápida y efectiva ante un incidente de seguridad.

En resumen, la ciberseguridad es una tarea compleja que requiere una combinación de tecnología, procesos y colaboración. Al invertir en soluciones de monitorización, automatización y comunicación, podemos mejorar significativamente nuestra capacidad de detectar y responder a amenazas.