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 alcance 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.
- **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.**

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

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 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.

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

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 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.

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

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 incumplimiento: 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.

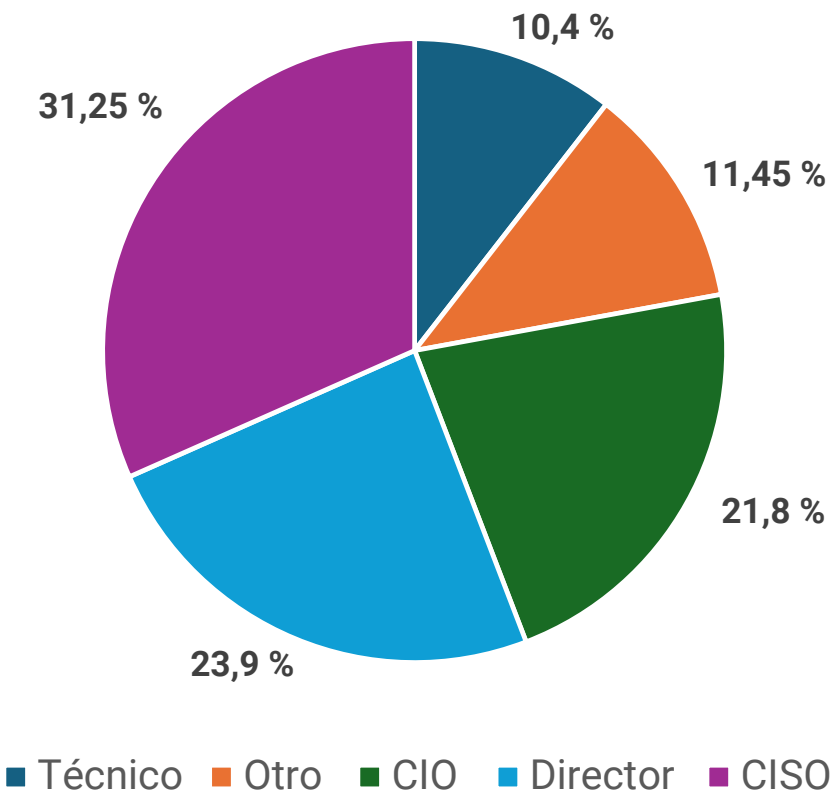
Destaca la participación de la figura del CISO, con un 31,25 % del total, seguida de la del director, con un 23,9 %.

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 %).

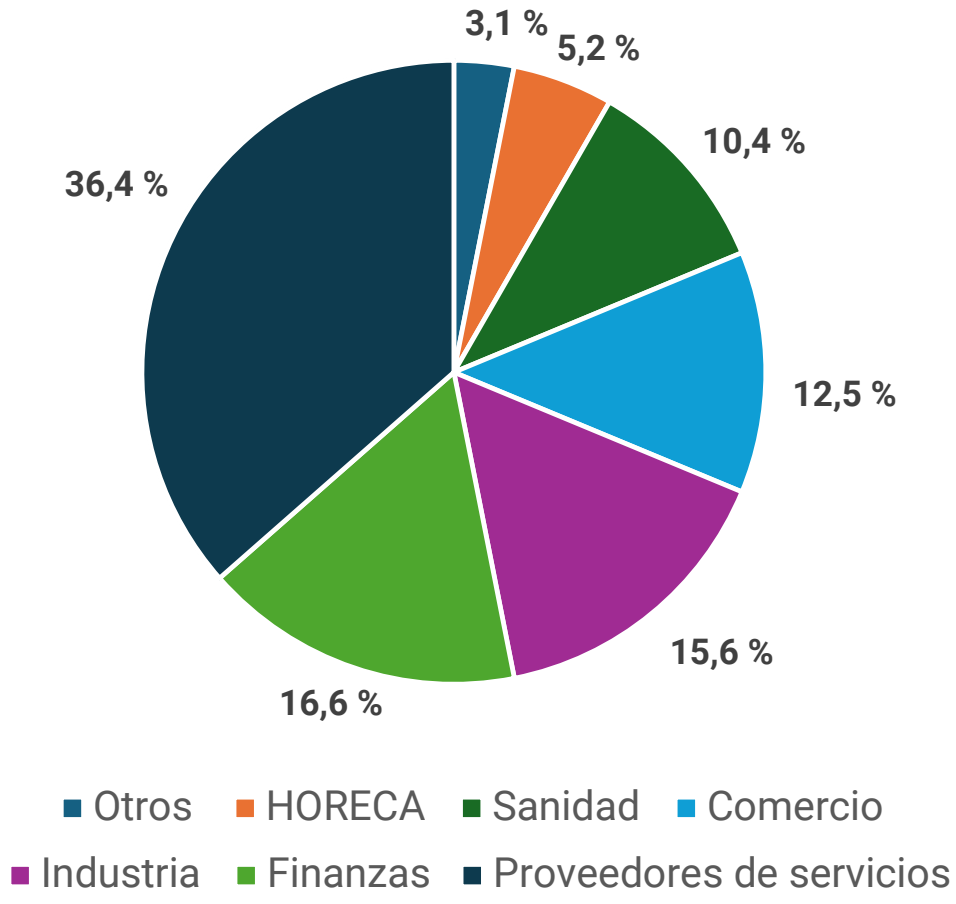
En cuanto los sectores de actividad de las empresas encuestadas, los proveedores de servicios son los más participativos, con un 36,4 % de total, seguido de finanzas (16,6 %), industria (15,6 %) y comercio (12,5 %).

Tipología de la muestra

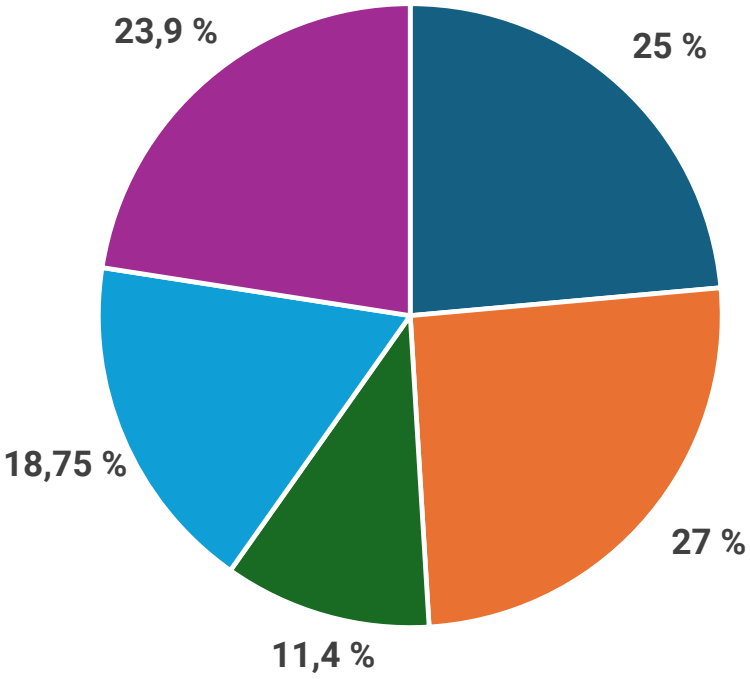
Perfil encuestados



Sector de actividad

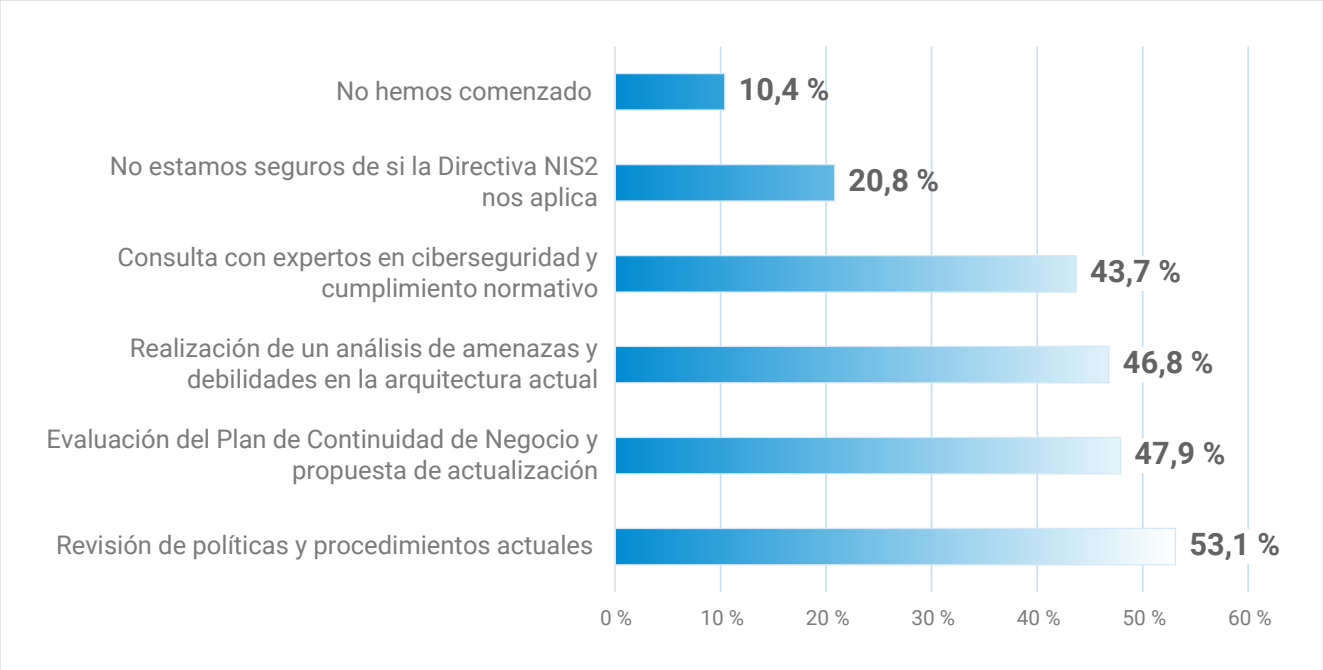


Tamaño de empresa



Resultados del estudio

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

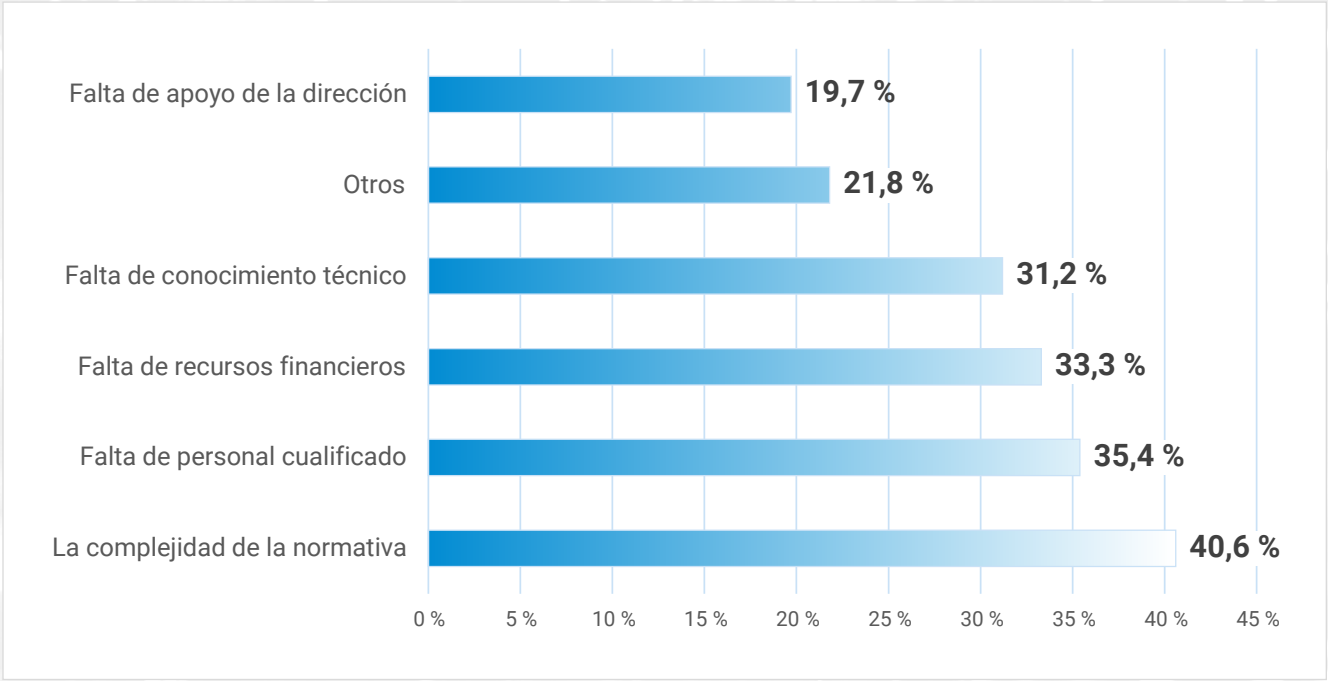


Antes de implementar una directiva hay que identificar si una organización está dentro del ámbito de aplicación de la misma, por lo que es fundamental llevar a cabo una evaluación.

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.

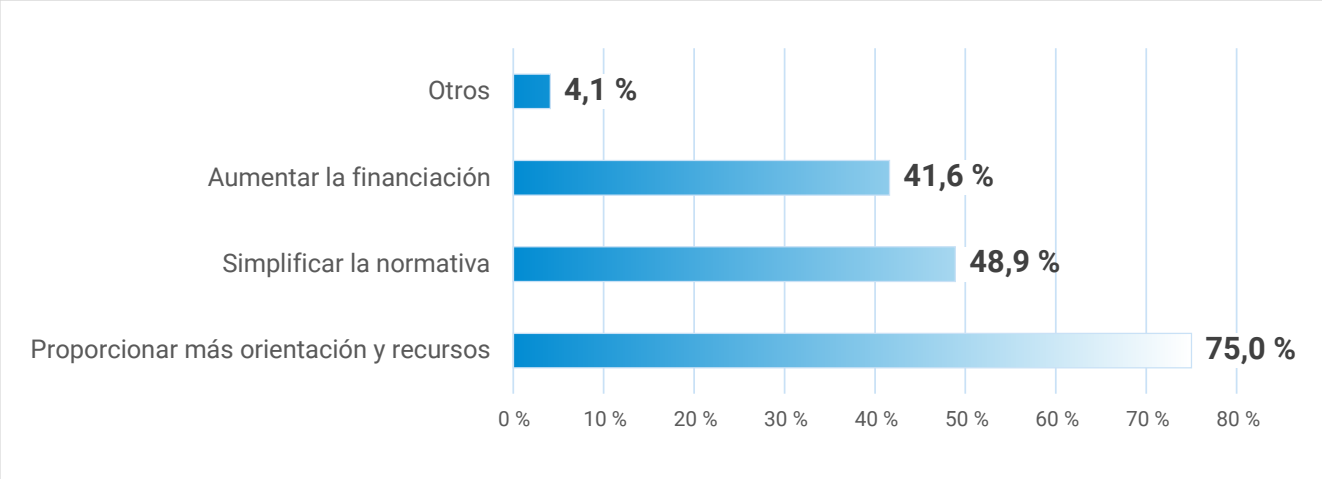
Las empresas que han iniciado el proceso de evaluación se han centrado principalmente en áreas como la revisión de políticas y procedimientos (53,1 %), la evaluación del **plan de continuidad del negocio** (47,9 %) o el análisis de amenazas y habilidades (46,8 %), lo que indica que reconocen la importancia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

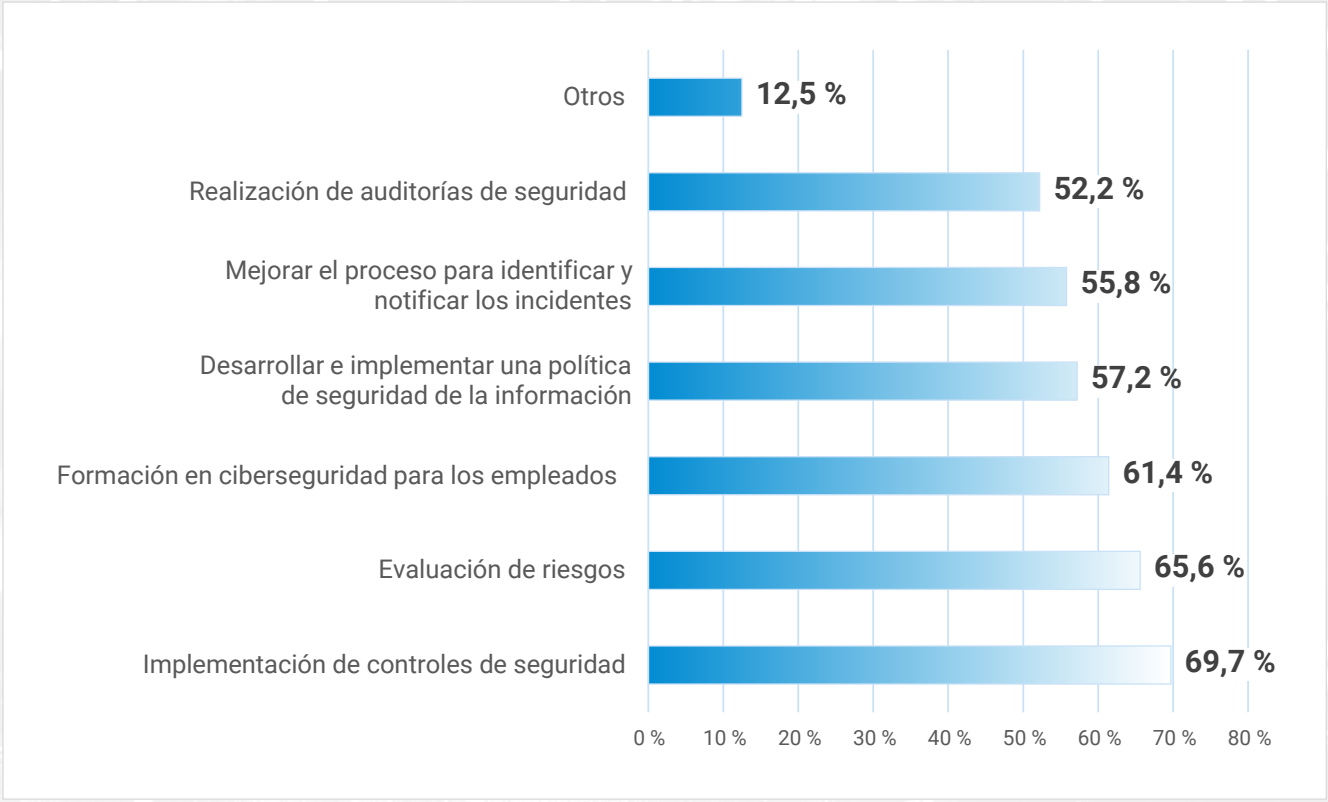
¿Qué medidas cree que las autoridades podrían tomar para facilitar la implementación de la Directiva NIS2 por parte de las empresas?



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.

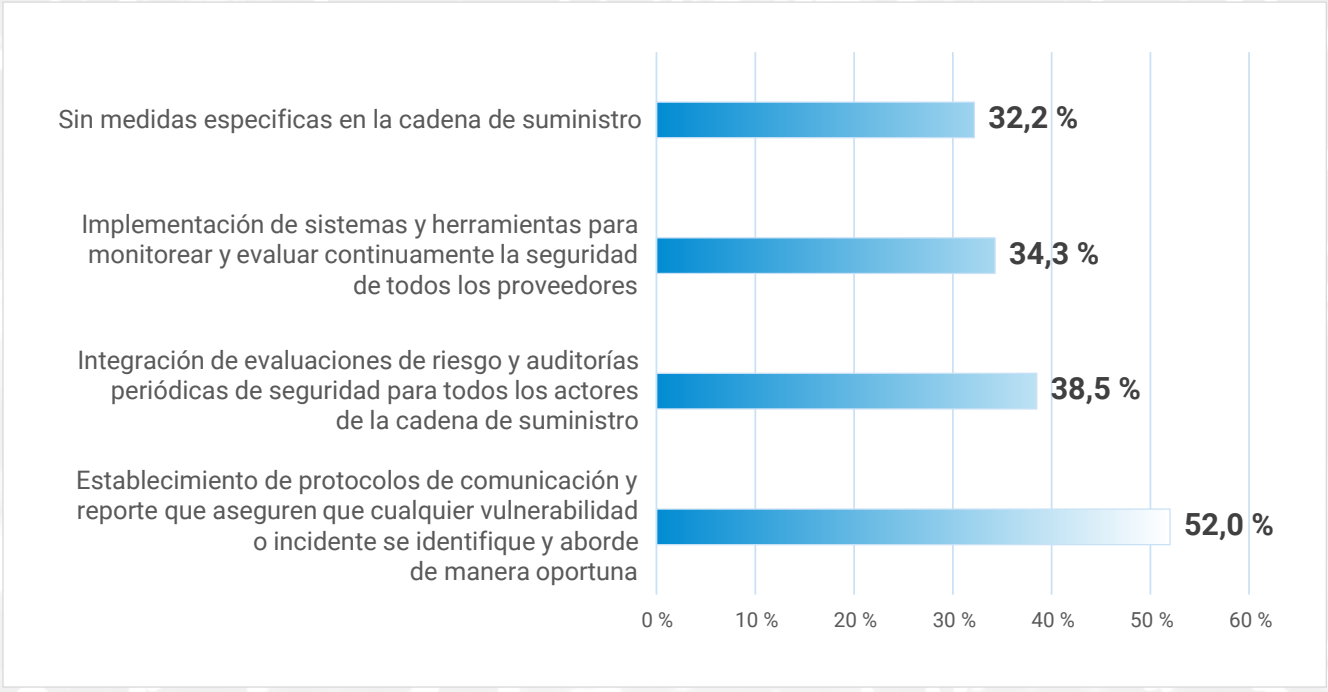
¿Qué medidas ha tomado su empresa para aumentar su ciberseguridad y prepararse para NIS2 en el último año?



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?



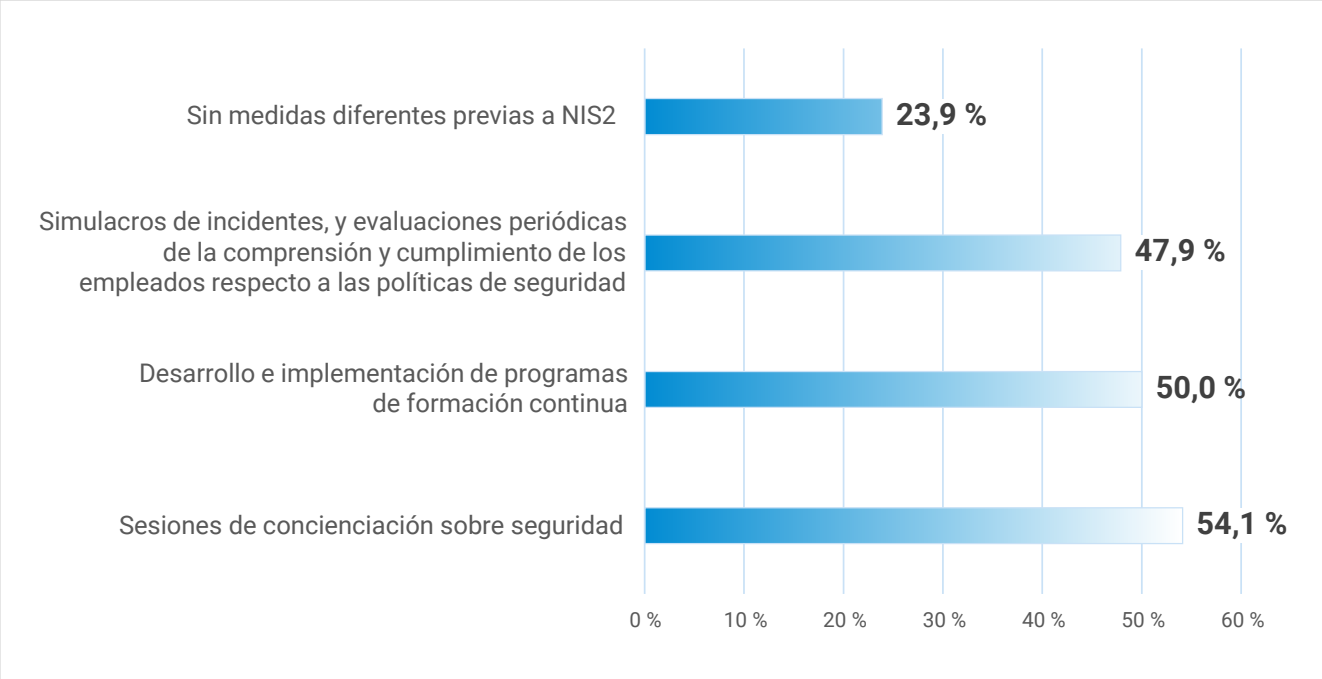
Una **visibilidad completa y continua en la cadena de suministro** protege a la empresa contra riesgos y amenazas, mejora su eficiencia, cumplimiento normativo y reputación.

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.

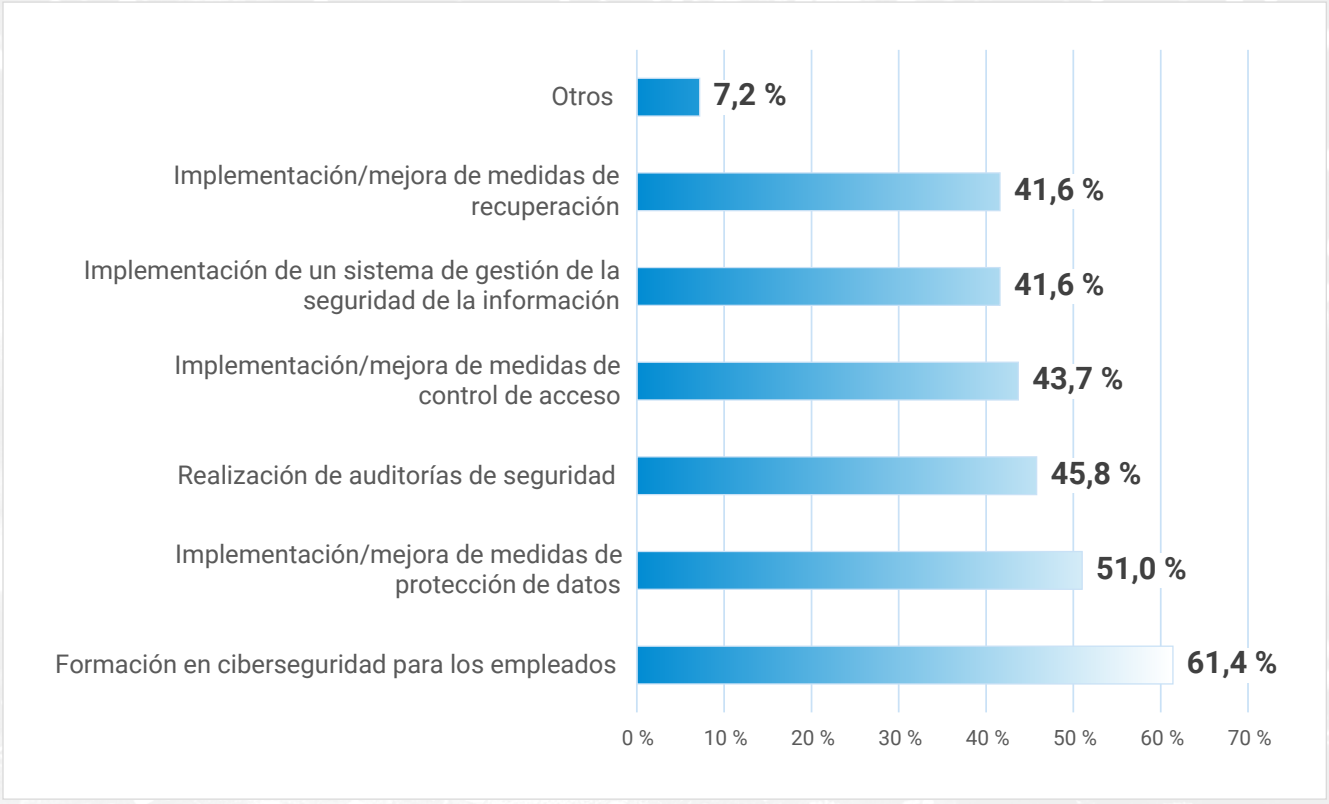
Por otra parte, un porcentaje significativo de empresas (32,2 %) **aún no cuenta con medidas específicas** para garantizar la visibilidad en su cadena de suministro, lo que representa un área de mejora.

¿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.

Plan de acción