Contacto: info@appluscertification.com

Certificación de la Directiva NIS2

¿Qué es la Directiva NIS2?

La **Certificación de la Directiva NIS2** (Network and Information System 2) se alza como una herramienta fundamental para fortalecer la ciberseguridad en la Unión Europea. Esta disposición legal, que entró en vigor el 16 de enero de 2023, establece un objetivo común para los países miembros: definir unos requisitos mínimos y armonizados para la protección de las infraestructuras críticas.

La Directiva NIS2 representa un paso adelante significativo en la lucha contra las ciberamenazas, sentando las bases para una Europa más segura y preparada para afrontar los desafíos del futuro digital.

Los Estados Miembros tienen hasta el **17 de octubre de 2024** para incorporar la Directiva NIS2 en sus legislaciones nacionales. Se estima que esta medida afectará a unas 160.000 entidades, las cuales deberán reforzar sus controles de seguridad para cumplir con los nuevos requisitos.

¿Cuáles son los objetivos de la Directiva NIS2?

Los objetivos de la Directiva NIS2 son los siguientes:

- Aumentar el nivel general de ciberseguridad en la UE.
- Mejorar la resiliencia de las redes y sistemas de información.
- Garantizar una respuesta más rápida y coordinada ante los incidentes cibernéticos.

¿Por qué es importante la NIS2?

Los requisitos de seguridad de la directiva NIS2 **son muy estrictos**, y un gran número de compañías de la Unión Europea (según unas estimaciones, aproximadamente más de 100.000) tendrán que cumplir con ella. Aunque no tendrá el mismo impacto que, por ejemplo, el RGPD de la UE, es muy probable que la NIS2 acabe convirtiéndose en un estándar que muchos países intentarán aplicar, del mismo modo que ocurrió con el RGPD.

¿Cuáles son los principales requisitos de ciberseguridad de la NIS2?

Para la correcta aplicación de la directiva NIS 2, hay una serie de requisitos que vale la pena tener en cuenta, y así evitar riesgos de ciberseguridad:

- Por parte del equipo de dirección, se deberán **aprobar las medidas de seguridad** que se crean convenientes, **supervisar su implementación** y, si las medidas no se implementan correctamente, **asumir responsabilidades**.
- Los miembros del equipo de dirección **deberán formarse en materia de ciberseguridad y ofrecer esta formación**, de una forma periódica, a sus empleados.
- Las medidas de ciberseguridad **deben ser apropiadas** para los riesgos correspondientes, considerando que la compañía debe tener en cuenta: la exposición a los riesgos, el tamaño de la entidad, la probabilidad que se produzcan incidentes y las repercusiones sociales y económicas de estos incidentes.
- Las compañías deberán **tomar las medidas técnicas, operativas y organizativas correspondientes** para gestionar riesgos y evitar o minimizar las repercusiones de los incidentes.
- Las compañías deberán **prestar especial atención a los riesgos relacionados con los proveedores** o prestadores de servicios directos, desde vulnerabilidades específicas de cada proveedor a procedimientos de desarrollo seguro de estos mismos.
- Las compañías deberán **notificar cualquier incidente significativo a los equipos de respuesta a incidentes de seguridad informática (CSIRT)**, mediante: una alerta temprana, una notificación del incidente, un informe intermedio, un informe final y un informe de situación.
- Aunque aún no es obligatorio, las compañías deberán **tener sus productos o servicios de TIC correctamente certificados**, de acuerdo con el esquema europeo de certificación de la ciberseguridad.
- Las compañías deberán **realizar inspecciones periódicas para evitar sanciones y multas**. Estas inspecciones van desde inspecciones in situ, supervisión a distancia, auditorías de ciberseguridad y escáneres de seguridad.

¿Cuáles son los beneficios de la Directiva NIS2?

Los beneficios de la Directiva NIS2 son los siguientes:

- **Incrementar la seguridad de los ciudadanos europeos**: Al proteger las infraestructuras críticas, como las redes energéticas o los sistemas sanitarios, se reduce el riesgo de ciberataques que podrían ocasionar graves perjuicios a la población.
- **Fomentar un entorno digital más confiable**: La confianza en el mundo digital es esencial para el desarrollo económico y social. La Directiva NIS2 contribuirá a crear un ecosistema digital más seguro y resiliente.
- **Fortalecer la ciberseguridad en el seno de la Unión Europea**: Se busca elevar el nivel de protección general frente a las ciberamenazas, cada vez más sofisticadas y frecuentes.
- **Fomentar la cooperación internacional**: La lucha contra los ciberataques requiere un frente unido. La Directiva NIS2 promueve el intercambio de información y la colaboración entre países y socios a nivel global.

¿A quién va dirigida la Directiva NIS2?

Según su **tamaño**, la Directiva NIS2 se aplicará en general a medianas y grandes compañías, pero no a las más pequeñas. En concreto en el ámbito de la mediana empresa, serán aquellas entre 50 y 250 empleados, y entre 10 y 50 millones de euros de ingresos anuales.

En cuanto a los **sectores**, estas son algunas de las categorías de entidades que están obligadas a cumplir con la NIS2:

- **Operadores de Servicios Esenciales (OSE)**: Incluye empresas y organizaciones que desempeñan servicios cruciales en sectores como energía (electricidad, petróleo, gas), transporte (aéreo, ferroviario, por agua y carretera), banca, infraestructuras del mercado financiero, salud, suministro y distribución de agua potable, y seguridad digital.
- **Proveedores de Servicios Digitales Importantes (PSDI)**: Abarca a los proveedores de servicios en la nube, motores de búsqueda en línea y servicios de redes sociales, ampliando el enfoque más allá de los proveedores de servicios digitales contemplados en la NIS original.
- **Administraciones Públicas**: La directiva sugiere que los Estados miembros consideren la inclusión de entidades de la administración pública dentro del alcance de la directiva, debido a su papel en la prestación de servicios esenciales y en la gestión de información sensible.
- **Otras entidades**: La NIS2 también trae bajo su alcance a otras entidades consideradas importantes para la economía y la sociedad, basándose en su tamaño y el impacto potencial que un incidente cibernético podría tener sobre la seguridad pública y económica.

¿Por qué elegir Applus+ Certification para la certificación de la Directiva NIS2?

Applus+ Certification es una entidad independiente y de reconocido prestigio que tiene por objetivo ayudar a las organizaciones a alcanzar su compromiso de mejora continua.

Analizamos las necesidades de los clientes para que nuestros auditores, especialistas en cada sector de actividad, desempeñen un servicio que aporte el máximo valor a la hora de evaluar la conformidad en su organización.

Nuestros equipos desarrollan planes específicos de certificación en función de la estructura, los procesos y las actividades de nuestros clientes.

Nuestra presencia internacional, nuestro extenso portafolio de productos y nuestras acreditaciones nos permiten prestar un servicio global, experto y adaptado a las necesidades de su organización.