Contact: info@appluscertification.com

NIS2 Directive Certification

What is the NIS2 Directive?

The **NIS2 Directive Certification** (Network and Information System 2) stands as a fundamental tool to strengthen cybersecurity in the European Union. This legal provision, which entered into force on 16 January 2023, establishes a common objective for member countries: to define minimum and harmonised requirements for the protection of critical infrastructures.

The NIS2 Directive represents a significant step forward in the fight against cyber threats, laying the foundations for a more secure Europe that is ready to face the challenges of the digital future.

Member States have until **17 October 2024** to transpose the NIS2 Directive into national law. It is estimated that this measure will affect around 160,000 entities, which will have to strengthen their security controls to comply with the new requirements.

What are the objectives of the NIS2 Directive?

The objectives of the NIS2 Directive are as follows:

- To increase the overall level of cybersecurity in the EU.
- To improve the resilience of networks and information systems.
- To ensure a faster and more coordinated response to cyber incidents.

Why is NIS2 important?

The security requirements of the NIS2 directive **are very strict**, and a large number of companies in the European Union (by some estimates, approximately more than 100,000) will have to comply with it. Although it will not have the same impact as, for example, the EU's GDPR, it is very likely that NIS2 will eventually become a standard that many countries will try to implement, in the same way as the GDPR did.

What are the main cybersecurity requirements of NIS2?

For the correct implementation of the NIS 2 directive, there are a number of requirements that are worth taking into account in order to avoid cybersecurity risks:

- On the part of the management team, **security measures that are deemed appropriate must be approved**, their implementation must be monitored and, if the measures are not implemented correctly, **responsibilities must be assumed**.
- Members of the management team **should be trained in cybersecurity and provide this training to their employees** on a regular basis.
- Cybersecurity measures should be appropriate to the risks involved, taking into account the company's exposure to the risks, the size of the entity, the likelihood of incidents occurring, and the social and economic impact of such incidents.
- Companies should **take appropriate technical, operational and organisational measures** to manage risks and avoid or minimise the impact of incidents.
- Companies should **pay particular attention to risks related to direct suppliers** or service providers, ranging from supplier-specific vulnerabilities to secure supplier development procedures.
- Companies should **report any significant incidents to the Computer Security Incident Response Teams (CSIRTs)**, through: an early warning, an incident notification, an interim report, a final report and a status report.
- Although not yet mandatory, companies should **have their ICT products or services properly certified**, in accordance with the European Cybersecurity Certification Scheme.
- Companies will have to **carry out regular inspections to avoid sanctions and fines**. These inspections range from on-site inspections, remote monitoring, cybersecurity audits and security scans.

What are the benefits of the NIS2 Directive?

The benefits of the NIS2 Directive are as follows:

- **Increasing the security of European citizens**: By protecting critical infrastructures, such as energy grids or healthcare systems, the risk of cyber-attacks that could cause serious harm to the public is reduced.

- **Fostering a more trustworthy digital environment**: Trust in the digital world is essential for economic and social development. The NIS2 Directive will contribute to creating a more secure and resilient digital ecosystem.
- **Strengthening cybersecurity within the European Union**: The aim is to raise the overall level of protection against increasingly sophisticated and frequent cyber threats.
- **Promoting international cooperation**: The fight against cyber-attacks requires a united front. The NIS2 Directive promotes information sharing and collaboration between countries and partners globally.

Who is the NIS2 Directive aimed at?

According to companies **size**, NIS2 will generally apply to medium and large companies, but not to smaller ones. Specifically in the field of medium-sized companies, they will be those with between 50 and 250 employees, and between 10 and 50 million euros in annual revenue.

By **sectors**, these are some of the categories of entities that are obliged to comply with the NIS2:

- **Essential Service Operators (ESO)**: includes companies and organisations that perform crucial services in sectors such as energy (electricity, oil, gas), transport (air, rail, water and road), banking, financial market infrastructure, health, drinking water supply and distribution, and digital security.
- **Major Digital Service Providers (ISPs)**: Covers cloud service providers, online search engines and social networking services, broadening the focus beyond the digital service providers covered in the original NIS.
- **Public administrations**: The directive suggests that Member States consider including public administration entities within the scope of the directive, due to their role in providing essential services and managing sensitive information.
- **Other entities**: The NIS2 also brings under its scope other entities considered important to the economy and society, based on their size and the potential impact a cyber incident could have on public and economic security.

Why choose Applus+ Certification for NIS2 Certification?

Applus+ Certification is an independent and reputable organisation that aims to help organisations achieve their commitment to continuous improvement.

We analyse our clients' needs so that our auditors, specialists in each sector of activity, can provide a service that provides maximum value when assessing your organisation's compliance.

Our teams develop specific certification plans based on our Clients' structure, processes and activities.

Applus certification

Our international presence, extensive product portfolio and accreditations enable us to provide a global, expert service tailored to your organisation's needs.