WEBINAR, 30 DE JULIO

CONOCE TODO SOBRE LA DIRECTIVA NIS2 Y EL ESQUEMA NACIONAL DE SEGURIDAD

CÓMO AFECTARÁ A PARTIR DEL 18 DE OCTUBRE

Con la participación de **Miguel Hernández**, CEO de Audinfor System, **David López** asesor experto en ciberseguridad y cumplimiento (ENS/NIS2) y **Daniel Serna**, socio director del Área de Derecho Público Lacasa Abogados, Palacios & Partners.

audinfor system M2D CONSULTORÍA

CONOCE TODO SOBRE LA DIRECTIVA NIS2 Y EL ESQUEMA NACIONAL DE SEGURIDAD

Miguel Hernández, CEO de Audinfor System

Daniel Serna, socio director del Área de Derecho Público Lacasa Abogados, Palacios & Partners

David López, M2D Consultoría, asesor experto en ciberseguridad y cumplimiento (ENS/NIS2)

audinfor system M2D CONSULTORÍA

ÍNDICE

1. Introducción

DIRECTIVA DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

La **Directiva (UE) 2022/2555,** conocida como NIS2, establece obligaciones de ciberseguridad para los Estados miembros y medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación.

¿A quién se le aplica? La Directiva NIS2 se aplica a sectores como la **energía**, el transporte o la sanidad. Son los llamados **Operadores de Servicios Esenciales**, que deben aplicar medidas de gestión de riesgos para garantizar la seguridad de sus sistemas informáticos. **Esto afecta a todas las empresas energéticas.**

Fecha de entrada en vigor: el cumplimiento de la **Directiva NIS2** va a ser de obligado cumplimiento a partir del **18 de octubre de 2024**. Para evitar multas y otros inconvenientes, las empresas deben comprender la Directiva NIS2, identificar sus posibles deficiencias y trabajar constantemente en fortalecer sus **medidas de ciberseguridad** para cumplir con los estrictos estándares de NIS2.

ÁMBITO LEGAL

2. ¿Qué es la Directiva NIS2?

7 IDEAS QUE RESUMEN LA DIRECTIVA NIS2 (DIRECTIVA (UE) 2022/2555)

1. Incremento del nivel común de ciberseguridad en la Unión Europea: la NIS2 busca garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea. Esto implica el establecimiento de marcos nacionales de seguridad, estrategias nacionales, y capacidades nacionales de ciberseguridad para proteger los sistemas de redes y de información utilizados en sectores críticos, exigiendo a las empresas afectadas la incorporación de requisitos de seguridad más estrictos para una mejor gestión de riesgos.

2. Ampliación del ámbito de aplicación y eliminación de diferencias entre Estados miembros: la directiva amplía su ámbito de aplicación a más sectores y servicios críticos, eliminando las grandes divergencias en la aplicación entre los Estados miembros, e impactando directamente en todas aquellas empresas del sector energía. Esto busca una mayor armonización y cooperación a nivel de la Unión, evitando la fragmentación del mercado interior y aumentando la ciber resiliencia.

3. Configuración de régimen jurídico en función de la calificación de la entidad: la directiva establece un claro criterio de distinción entre entidades esenciales e importantes, en función, entre otros de la inclusión de la tipología de la actividad dentro de alguno de los anexos de la Directiva. A título descriptivo, una entidad importante será una organización que, aunque no es crítica, su interrupción podría afectar la economía o la seguridad pública (fabricación, gestión de residuos y los servicios digitales, etc.). Por su parte, una entidad esencial será una organización cuya interrupción tendría un impacto significativo en la economía o la sociedad, como son los sectores de energía, transporte, salud y agua potable. Hay que tener en cuenta que, con fecha límite el 17 de abril de 2025, los Estados miembros deberán elaborar una lista de entidades esenciales e importantes para su comunicación a la Comisión.

2. ¿Qué es la Directiva NIS2?

7 IDEAS QUE RESUMEN LA DIRECTIVA NIS2 (DIRECTIVA (UE) 2022/2555)

4. Fortalecimiento de la cooperación y la respuesta coordinada: la NIS2 refuerza la cooperación entre los Estados miembros y establece mecanismos para la respuesta coordinada a incidentes de ciberseguridad a gran escala. Incluye la participación de la Red europea de organizaciones de enlace nacionales para las crisis de ciberseguridad (EU-CyCLONe) y el Grupo de Cooperación para garantizar una respuesta efectiva y coordinada.

5. Promoción de la ciberhigiene y la sensibilización en ciberseguridad: la directiva destaca la importancia de las políticas de ciberhigiene, que incluyen prácticas básicas como actualizaciones de software y hardware, cambios de contraseñas y gestión de accesos. También subraya la necesidad de aumentar la sensibilización sobre ciberseguridad para mejorar la protección contra ciberamenazas.

6. Fomento de la innovación y adopción de tecnologías avanzadas: la NIS2 promueve el uso de tecnologías innovadoras, incluida la inteligencia artificial, para mejorar la detección y prevención de ciberataques. También fomenta el uso de herramientas de ciberseguridad de código abierto para incrementar la transparencia y eficiencia en la innovación industrial, beneficiando especialmente a las pequeñas y medianas empresas.

7. Control de cumplimiento de los requisitos de la Directiva: los Estados miembros tienen de margen hasta el día 17 de enero de 2025 para comunicar a la Comisión Europea qué régimen sancionador van a aplicar en caso de incumplimiento de la NIS2. Si bien la Directiva fija como referencias para las entidades esenciales de 10.000.000 € o un máximo de un 2% del volumen de negocio anual total a nivel mundial del ejercicio financiero anterior y, para las entidades importantes, de 7.000.000 € o un máximo de un 1.4% del volumen de negocio anual total a nivel mundial del ejercicio financiero anterior.

ÁMBITO OPERATIVO

CAPÍTULO IV

Artículo 20 - Gobernanza

Artículo 21 - Medidas para la gestión de riesgos de ciberseguridad

Artículo 23 - Obligaciones de notificación

Artículo 24 - Utilización de esquemas europeos de certificación de la ciberseguridad

3.1 Capítulo IV:

Artículo 20 - Gobernanza

Los órganos de dirección deben aprobar las medidas para:

- La gestión de riesgos de ciberseguridad adoptadas por dichas entidades para dar cumplimiento al artículo 21,
- Supervisen su puesta en práctica y
- Respondan por el incumplimiento por parte de las entidades de dicho artículo

Los miembros de los órganos de dirección deben asistir a formaciones periódicamente al objeto de adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.

Alentarán a estas entidades para que ofrezcan formaciones similares a sus empleados.

3.2 Capítulo IV:

Artículo 21 – Medidas para la gestión de riesgos de ciberseguridad

Las empresas deben tomar medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de los sistemas de redes y de información que usan en sus operaciones o en la prestación de sus servicios para prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios.

Las medidas incluirán **al menos** los siguientes elementos:

a) las políticas de seguridad de los sistemas de información y análisis de riesgos;

b) la gestión de incidentes;

c) la continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis;

d) la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos;

e) la seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades;

f) las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad;

g) las prácticas básicas de ciberhigiene y formación en ciberseguridad;

h) las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado;

i) la seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos;

j) el uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

3.3 Capítulo IV:

Artículo 23 – Obligaciones de notificación

Cada Estado miembro velará por que:

- Las entidades esenciales e importantes notifiquen, sin demora indebida, a su CSIRT o, en su caso, a su autoridad competente cualquier **incidente** que tenga un impacto significativo
- Las entidades esenciales e importantes comuniquen, sin demora indebida, a los destinatarios de sus servicios que **puedan verse afectados por una ciberamenaza significativa** las medidas o soluciones que dichos destinatarios pueden aplicar en respuesta a la amenaza

(El flujo es muy preciso y tiene fechas concretas de cumplimiento de ciertos trámites e informes.)

3.4 Capítulo IV:

Artículo 24 – utilización de esquemas europeos de certificación de la ciberseguridad

A los efectos de demostrar la conformidad con determinados requisitos del artículo 21, los Estados miembros podrán exigir a las entidades esenciales e importantes que **utilicen productos, servicios** y procesos de TIC particulares que estén certificados en virtud de un esquema europeo de certificación de la ciberseguridad.

RELACIÓN ENTRE LA NIS2 Y EL ENS

4. Relación entre la NIS2 y ENS

LA NIS2 **no** se certifica

Artículo 24 – *utilización de esquemas europeos de certificación de la ciberseguridad*

En España

ESQUEMA NACIONAL DE SEGURIDAD
RD311/2022

De obligado cumplimiento para todo el **Sector Público** español.
También para todas las empresas **TI** que quieran trabajar para el Sector Público.

El ENS **sí** que se certifica/audita (cada dos años).

El ENS es **muy exigente** desde el punto de vista técnico y de la gestión de la seguridad de la tecnología y su mantenimiento.

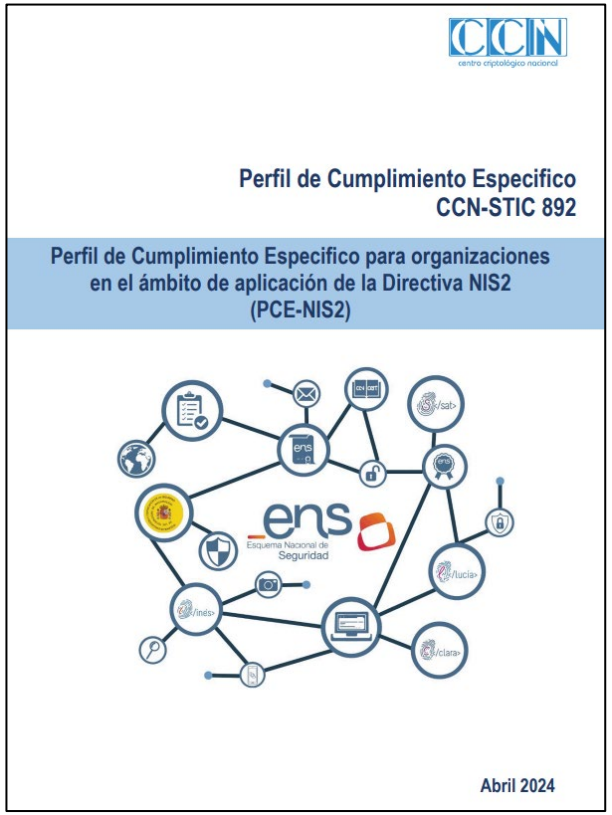
4. Relación entre la NIS2 y el ENS

EN BÉLGICA YA HAY TRASPOSICIÓN

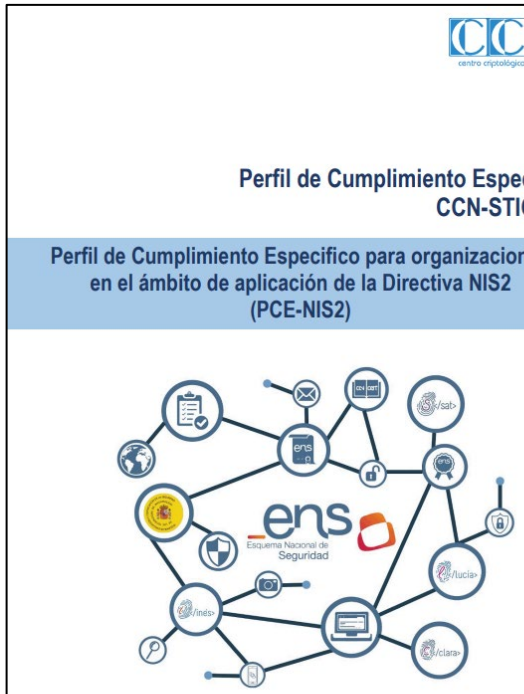
La NIS2 -> *CyberFundamentals Framework* (el ENS español)

EN ESPAÑA

No hay aún transposición, pero…



4. Relación entre la NIS2 y el ENS



Medida	Importantes	Esenciales	Aplicación[1]	Ref
org.1	SI	SI	BÁSICA	
org.2	SI	SI	BÁSICA	
org.3	SI	SI	BÁSICA	
org.4	SI	SI	BÁSICA	
op.pl.1	SI *	SI	MEDIA	71
op.pl.2	SI	SI	MEDIA	
op.pl.3	SI	SI	BÁSICA	
op.pl.4	SI	SI	Bajo	
op.pl.5	SI	SI	MEDIA (+R1+R2)	7.2
op.acc.1	SI	SI	Medio	
op.acc.2	SI	SI	Alto	
op.acc.3	SI	SI	Medio	
op.acc.4	SI	SI	Bajo	
op.acc.5	SI *	SI	Medio	7.3
op.acc.6	SI *	SI	Medio	7.4
op.exp.1	SI*	SI	BÁSICA (+R1+R2+R3+R4)	7.5
op.exp.2	SI	SI	BÁSICA	
op.exp.3	SI	SI	MEDIA	
op.exp.4	SI	SI	BÁSICA (+R4)	7.6
op.exp.5	SI	SI	MEDIA	
op.exp.6	SI	SI	MEDIA	
op.exp.7	SI	SI	ALTA	
op.exp.8	SI	SI	Medio	
op.exp.9	SI	SI	BÁSICA	
op.exp.10	SI	SI	BÁSICA	
op.ext.1	SI	SI	MEDIA	
op.ext.2	SI	SI	MEDIA	
op.ext.3	SI	SI	ALTA (+R1+R2+R3)	7.7
op.ext.4	SI	SI	ALTA	
op.nub.1	SI	SI	ALTA	
op.cont.1	SI	SI	Alto	
op.cont.2	SI	SI	Alto (+R1+R2)	7.8

Medida	Importantes	Esenciales	Aplicación[1]	Ref
op.cont.3	SI	SI	Alto	
op.cont.4	SI	SI	Alto (+R1)	7.9
op.mon.1	SI	SI	MEDIA	
op.mon.2	SI	SI	ALTA	
op.mon.3	SI *	SI	BÁSICA (+R2+R6)	7.10
mp.if.1	SI	SI	MEDIA	
mp.if.2	SI	SI	MEDIA	
mp.if.3	SI	SI	MEDIA	
mp.if.4	SI	SI	Medio	
mp.if.5	SI	SI	Medio	
mp.if.6	SI	SI	Medio	
mp.if.7	SI	SI	MEDIA	
mp.per.1	SI *	SI	MEDIA (R1)	711
mp.per.2	SI	SI	ALTA	
mp.per.3	SI	SI	BÁSICA	
mp.per.4	SI	SI	BÁSICA	
mp.eq.1	SI	SI	BÁSICA	
mp.eq.2	SI	SI	Medio	
mp.eq.3	SI	SI	MEDIA (R1)	7.12
mp.eq.4	SI	SI	Bajo	
mp.com.1	SI	SI	BÁSICA	
mp.com.2	SI	SI	ALTO (R4+R5)	7.13
mp.com.3	SI	SI	Medio	
mp.com.4	SI	SI	MEDIA	
mp.si.1	SI	SI	Medio	
mp.si.2	SI	SI	Alto	
mp.si.3	NO	SI	BÁSICA	
mp.si.4	NO	SI	BÁSICA	
mp.si.5	SI	SI	Bajo	
mp.sw.1	SI	SI	MEDIA	
mp.sw.2	SI	SI	BÁSICA	
mp.info.1	SI	SI (DNS)	BÁSICA	7.14
mp.info.2	NO	NO	N/A	
mp.info.3	NO	SI (PSC)	Alto	7.15
mp.info.4	NO	SI (PSC)	Alto	7.16
mp.info.5	SI	NO	Bajo	
mp.info.6	SI	SI	Alto	
mp.s.1	SI	SI	BÁSICA	
mp.s.2	SI	SI	MEDIA	
mp.s.3	SI	SI	MEDIA	
mp.s.4	SI	SI* (DNS)	Alto	5.17

INTEGRACIÓN DE LA NIS2/ENS

5. Integración de la NIS2/ENS (algunas claves)

¿Dos opciones?

Cumplir como sea y olvidarme hasta dentro de dos años ✗

Ya que hay que cumplir, aprovecharlo para dinamizar los procesos internos ✓

Se certifican los **servicios** prestados, no a las empresas en global.

Es importante acotarlo bien para no incurrir en gastos o trabajo extra.

Los proveedores certificados, facilitan el propio cumplimiento.

P.e.: La certificación de los servicios prestados por **Audinfor** agiliza y facilita la de sus clientes.

audinfor system

La NIS2/ENS genera carga de trabajo sobre quien gestiona la **infraestructura tecnológica**.

El uso de servicios en nube certificados facilita el propio cumplimiento, tb contratar proveedores certificados que accedan a nuestra infraestructura TI.

La NIS2/ENS abarca la **gestión de la seguridad** de los PCs, los móviles, los equipos de comunicaciones, los servidores, las salas técnicas, la gestión de las incidencias, la gestión de las vulnerabilidades, la gestión de los cambios, la realización de ataques simulados, el mantenimiento de los sistemas operativos, la gestión de la toma de decisiones sobre ciberseguridad, la gestión de los accesos, la gestión de los permisos, etc. etc. etc.

VENTAJAS DEL CUMPLIMIENTO DE LA NIS2/ENS

6. Ventajas del cumplimiento de la NIS2/ENS

Generación de confianza

Mejora en la relación con el cliente y los proveedores

Mejora y agilización de los procesos internos

Mejoras operativas

Mejora en la estandarización de la tecnología y la seguridad (mismo vocabulario)

Resoluciones más ágiles
Mejor integración con proveedores/clientes

La ciberseguridad mejora en los niveles de gobierno y gestión de la tecnología

Inclusión de la tecnología en la toma de decisiones

Mejor encaje en una seguridad global (Autonómico/Nacional)

Mayores niveles de protección sin incrementar costes

RONDA DE PREGUNTAS

audinfor system