DIRECTIVA NIS2:
REGULACIÓN DE CIBERSEGURIDAD PARA TU EMPRESA

CONSEJO ANDALUZ DE CÁMARAS DE COMERCIO, INDUSTRIA Y NAVEGACIÓN DE ANDALUCÍA

Junta de Andalucía
Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa

Cámaras Andalucía

enterprise europe network

Red de Información Europea de Andalucía

Estrella Freire Martín
Secretaria General Cámaras Andalucía

Bienvenida

Junta de Andalucía
Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa

Cámaras Andalucía

enterprise europe network

Red de Información Europea de Andalucía

Adrián Espina Barrera.
Abogado especializado en delitos digitales

ADRIÁN ESPINA
ABOGADO

Junta de Andalucía
Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa

Cámaras Andalucía

enterprise europe network

Red de Información Europea de Andalucía

ANTECEDENTES: DIRECTIVA NIS - NIS1

Año 2016: entrada en vigor Directiva (UE) 2016/1148 - DIRECTIVA NIS.

- Objetivo: fijación de criterios de seguridad para todos los EEMM.

España: transposición con el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

- Desarrollo: mediante Real Decreto 43/2021, de 26 de enero.

¿FUNCIONÓ LA DIRECTIVA NIS1?

Contexto:

- Rápida evolución tecnológica. Irrupción del “fenómeno blockchain” y del “Metaverso”.
- Aparición de nuevos riesgos para la ciberseguridad.

¿Qué fue mal?

- Aplicación desigual por los EEMM.
- Problemas de ciberseguridad y obstáculos jurídicos para las empresas que operaban en distintos EEMM.
- Riesgo para la armonía del Mercado Digital Único.

SOLUCIÓN: ELABORACIÓN Y APROBACIÓN DIRECTIVA NIS2

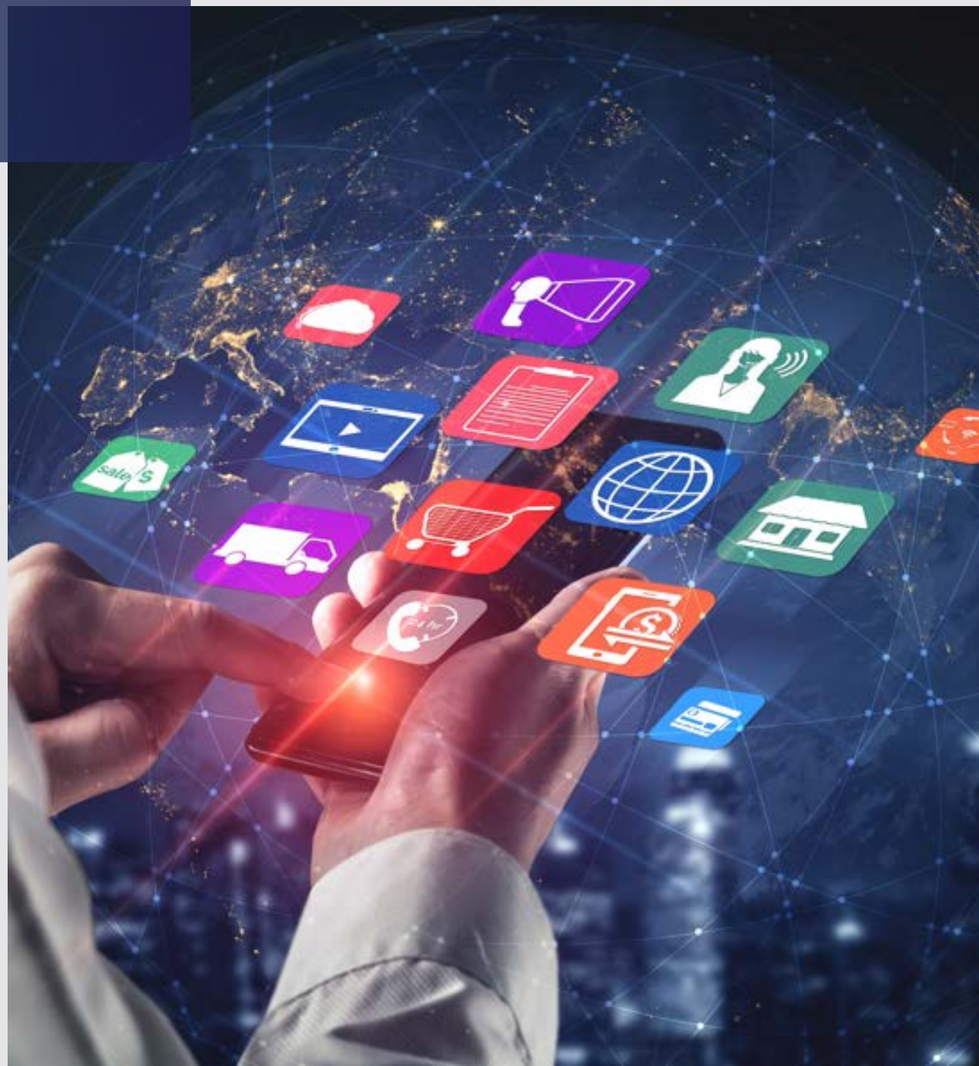
DIRECTIVA (UE) 2022/2555

Aprobada: 27 de diciembre de 2.022

Entrada en vigor: 16 de enero de 2.023

Plazo de transposición: hasta el 17/10/2024

España: seguimos esperando



OBJETIVOS DE LA DIRECTIVA NIS2

Artículo 1:

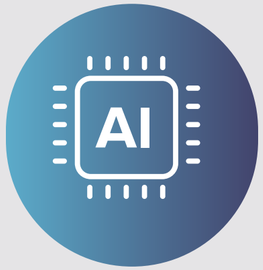
- Alcanzar un elevado nivel común de ciberseguridad en toda la Unión Europea.

- Que las empresas que operen en la UE gestionen adecuadamente los riesgos de ciberseguridad.

Obliga a:

1. Elaboración estrategias nacionales de ciberseguridad
2. Medidas de gestión de riesgos para la ciberseguridad
3. Notificación de incidentes
4. Intercambio información sobre ciberseguridad
5. Supervisión y ejecución

ÁMBITO DE APLICACIÓN
(art. 2)



A NIVEL SECTORIAL

SECTORES DE ALTA CRITICIDAD (11)

- Energía
- Banca
- Infraestructura financieros
- Salud
- Transporte
- Aguas potables
- Infraestructura Digital
- Aguas residuales
- Administración Pública
- Gestión de servicios TIC
- Espacio

OTROS SECTORES CRÍTICOS (7)

mercados

- Investigación
- Química
- Servicios Postales
- Alimentación
- Proveedores Digitales
- Fabricación
- Gestión de residuos

ÁMBITO DE APLICACIÓN
(art. 2)

A NIVEL EMPRESARIAL

Aplicable a entidades públicas o privadas que:

- **+250 empleados**
- **Volumen anual +50M€**
- **Balance anual +43M€.**

2 tipos de entidades:

- **Entidades Esenciales**
- **Entidades Importantes**

INDEPENDIENTEMENTE DEL TAMAÑO

- **Proveedores redes públicas comunicación electrónica**
- **Prestadores servicios de confianza**
- **Prestadores de servicios registro nombres de dominio**
- **Entidades cuya perturbación tenga repercusiones sobre la seguridad pública**

ENTIDADES ESENCIALES Y ENTIDADES IMPORTANES

ESENCIALES
(Artículo 3.1)

- **Entidades pertenecientes a sectores de Alta Criticidad:**
  - **+250 empleados**
  - **+50M€ volumen negocio anual**
  - **+43M€ balance anual**
- **Prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel**
- **Proveedores de redes públicas de comunicaciones electrónicas**
- **Proveedores de servicios de comunicaciones electrónicas**
- **Entidades de la Administración pública**

IMPORTANTES
(Artículo 3.2)

- **Entidades pertenecientes a sectores de Alta Criticidad o a otros sectores críticos:**
  - **-250 empleados**
  - **-50M€ facturación**
  - **-43M€ balance anual**

ANTES DEL 17 DE ABRIL DE 2025 LOS ESTADOS MIEMBROS DEBEN ELABORAR UNA LISTA DE LAS ENTIDADES ESENCIALES E IMPORTANTES ASÍ COMO DE LAS ENTIDADES QUE PRESTAN SERVICIOS DE REGISTRO DE NOMBRES DE DOMINIO

ORGANISMOS NACIONALES Y EUROPEOS VINCULADOS A LA DIRECTIVA NIS 2

ÁMBITO NACIONAL

Autoridades nacionales

Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT)

Punto de acceso único

ÁMBITO EUROPEO

Grupo de cooperación

Red de CSIRTs

Red Europea de Organizaciones de Enlace para la Crisis de Ciberseguridad (EU-CyCLONe)

ÁMBITO NACIONAL

AUTORIDAD NACIONAL

Supervisión entidades esenciales e importantes mediante:

- Inspecciones
- Auditorias
- Imposición sanciones

ESPAÑA: aun no se ha determinado.

Hay que esperar hasta la transposición.

CSIRT

- Asistencia a entidades esenciales e importantes mediante ante incidentes
- Difusión de alertas
- Avisos sobre ciberamenazas y vulnerabilidades

PUNTO DE ACCESO ÚNICO

Permitir la cooperación transfronteriza entre todas las autoridades competentes

ÁMBITO EUROPEO

Grupo de Cooperación

Lo forman representantes de:

- EEMM
- Comisión Europea
- ENISA

Proporciona a las autoridades orientación en la transposición y aplicación Directiva

Políticas de divulgación de vulnerabilidades y ciberamenazas

Red de CSIRTs

Formado por:

- Representantes CSIRT de cada EM
- Representantes CERT-EU

Intercambio de información sobre:

- Incidentes
- Ciberamenazas
- Vulnerabilidades

EU-CyCLONe

Formado por:

- Autoridades Gestión de crisis de EEMM
- Comisión Europea

Respalda de manera coordinada los incidentes y crisis de ciberseguridad a gran escala

Gobernanza

Gestión de riesgos

Notificación de incidentes

Intercambio de información

Gobernanza

Artículo 20

Relevancia y responsabiliades Órganos Directivos

Aprobar y supervisar las medidas de gestión de riesgos de ciberseguridad. Sanción en caso de incumplimiento

Formación en materia de gestión de riesgos

Medidas de gestión de crisis

Artículo 21

Obligación de los Órganos Directivos de las entidades esenciales e importantes

Lista de medidas mínimas. Compatibles con otras medidas no previstas

Actitud proactiva, no reactiva

Supervisión y control periódico por el Órgano de Dirección

Medidas de gestión de crisis

Medidas a implementar:

- Políticas de seguridad de sistemas de información y análisis de riesgos
- Elaboración de proceso detallado y completo de gestión de incidentes
- Política de evaluación periódica de medidas adoptadas

Medidas de gestión de crisis

- Prácticas de ciberhigiene y formación en ciberseguridad
- Políticas y procesos enfocados en el uso de criptografía y cifrado
- Políticas de uso de recursos humanos
- Tecnología de autenticación multifactor o autenticación continuada

Notificación incidentes

Artículo 23

Obligación de las entidades esenciales e importantes de notificar al CSIRT o a la autoridad competente cualquier incidente que tenga “impacto significativo”

INCIDENTE CON IMPACTO SIGNIFICATIVO: aquel que cause o pueda causar gran perturbación operativa en los servicios y/o provoque pérdidas económicas para la entidad y afecte o pueda afectar a personas

Obligación de notificar a afectados

Notificación incidentes
Plazos

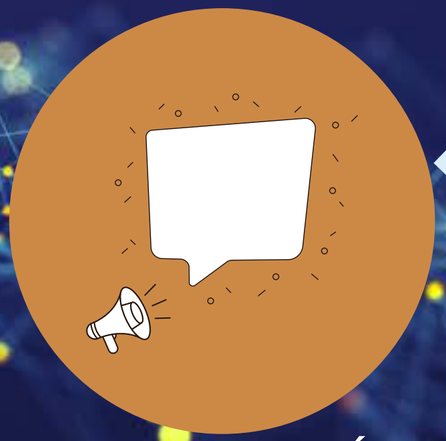
- Notificación al CSIRT o autoridad competente en 24 horas desde incidente. NOTIFICACIÓN TEMPRANA:
  - acción ilícita o malintencionada
  - Posible repercusión trasnfronteriza

- Tras 72 horas: informe sobre actualización del incindente. NOTIFICACIÓN INTERMEDIA:
  - Gravedad
  - Impacto

- Tras un mes (máximo) - NOTIFICACIÓN FINAL:
  - Descripción detallada del informe (gravedad e impacto)
  - Causa
  - Medidas para paliar daños
  - Posible implicaciones transfronterizas

INCIDENTE

NOTIFICACIÓN
TEMPRANA
24H MÁX



NOTIFICACIÓN
INTERMEDIA
72H MÁX

NOTIFICACIÓN
FINAL
MÁXIMO 1 MES

Intercambio de información

Artículo 29

Los EEMM deben proveer a las entidades esenciales e imortantes mecanismos de intercambio de información para:

- Prevenir, detectar o responder a incidentes
- Recuperarse de un incidente
- Mitigar su repercusión
- Reforzar el nivel de ciberseguridad
- Limitar la propagación de amenazas

Fomento de intercambio dentro de comunidades de entidades

RÉGIMEN SANCIONADOR

ART. 34

Incumplimiento arts. 21 y 23

- Efectividad
- Proporcionalidad
- carácter disuasorio

ART. 36

EEMM - plazo hasta 17 de enero de 2025 para:

- Desarollo régimen sancionador
- Comunicación a la Comisión

RÉGIMEN SANCIONADOR

TIPOLOGÍA

ESENCIALES

- Hasta 10M€
- 2% máx. volumen negocio anual total

IMPORTANTES

- Hasta 7M€.
- 1,4% máx. volumen negocio total anual

17/01/2023	17/10/2024	17/01/2025	17/04/2025	17/04/2027
Inicio plazo transposición	Fin plazo transposición	Fin plazo desarollo régimen sancionador	Fin plazo lista entidades esenciales e impotantes	Fin plazo para 1ª revisión Directiva

Turno de dudas y preguntas

Junta de Andalucía
Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa

Cámaras Andalucía

enterprise europe network

Red de Información Europea de Andalucía