Ciberseguridad
Impacto en operadores de transporte

AENOR ER Empresa Registrada UNE-EN ISO 9001 ER0023/2003
AENOR Gestión Ambiental UNE-EN ISO 14001 GA-2021/0462
AENOR ER Seguridad Información UNE-ISO/IEC 27001 SI 0003/2004
AENOR ER Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-0012/2009
AENOR Gestión Energética UNE-EN ISO 50001 GE-2021/0041
AENOR ER Gestión I+D+i UNE 166002 IDI-0003/2013
AENOR PRIVACIDAD INFORMACIÓN ISO 27701 PI-0001/2020

bsi. ISO 22301 Business Continuity Management BCMS 553603

CMMI DEV /3 SM Exp. 2019-04-22 / Appraisal #26155

gmv INNOVATING SOLUTIONS

íNDICE

Incidentes de ciberseguridad en sector transporte

El sector del transporte supone una tercera parte de los ciberdelitos en España

Actualidad 29 FEB 2024

it Digital Security

Este mensaje SMS con recordatorio de pago de una multa de la DGT es un fraude

rtve

El sector del transporte recibe un 25% de los ciberataques

el canal MARÍTIMO Y LOGÍSTICO

El ciberataque al consorcio de transportes de Madrid crea alerta en el sector

Por Mayte #CIBERSEGURIDAD

CARRIL BUS

Train passengers see terror messages after station wi-fi hack

Man arrested for 'cyber-vandalism' after 19 stations are affected by technology breach

THE TIMES

ticket sales stopped

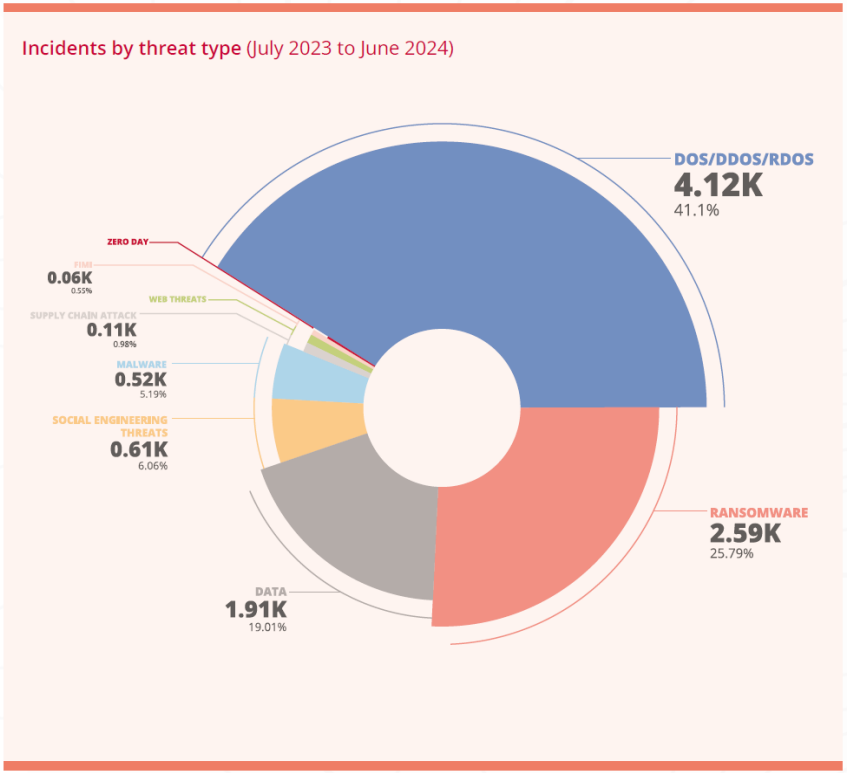
Cyberattack paralyzes airline

Bild

gmv

Principales tipos de incidentes de ciberseguridad

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL



Fuente: 2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION ENISA (EUROPEAN UNION AGENCY FOR CYBERSECURITY)

DOS/DDOS/RDOS: Ataques de denegación de servicio.

RANSOMWARE: Cifrado de archivos o sistemas y exigencia de un pago para restaurar el acceso.

DATA: Datos sensibles, confidenciales o personales son accedidos, expuestos, alterados, robados o destruidos sin autorización.

SOCIAL ENGINEERING THREATS: Manipulación para engañar a personas y hacer que revelen información confidencial o comprometan la seguridad de un sistema (phishing, baiting, ...)

MALWARE: SW diseñado para comprometer, infectar o dañar un sistema (virus, troyanos, ...)

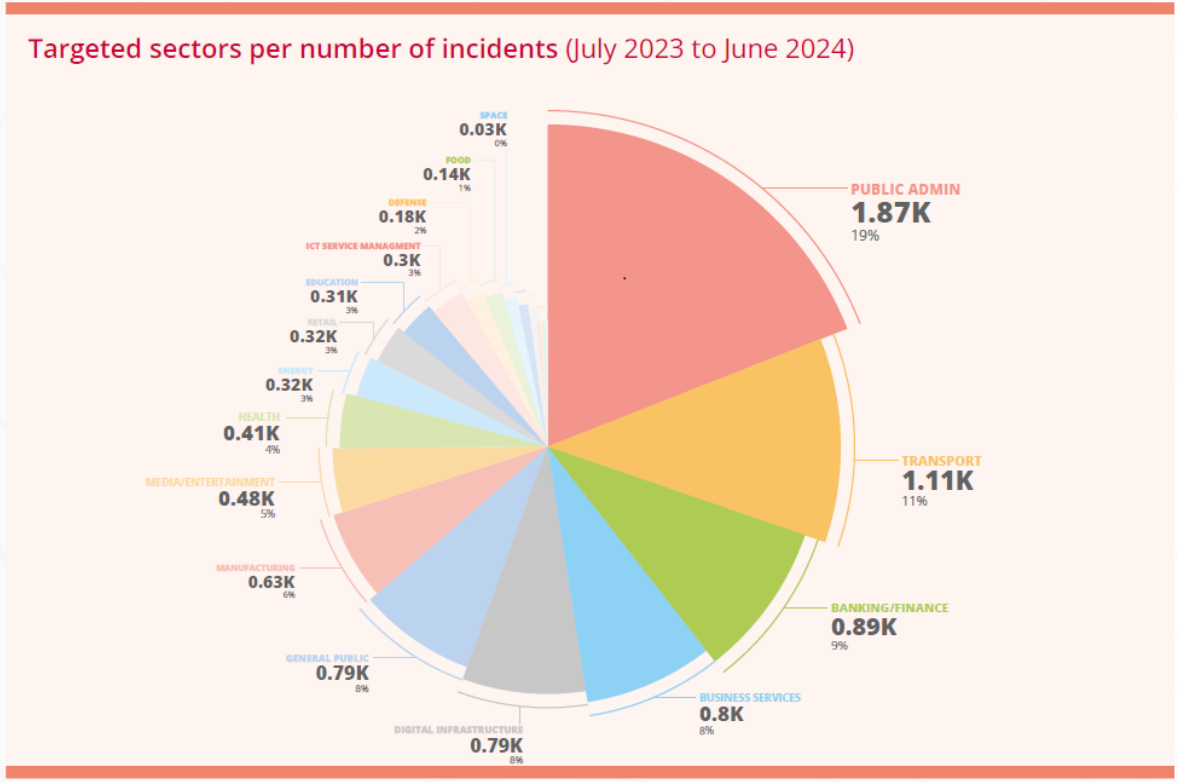
SUPPLY CHAIN ATTACK: Ataque para comprometer proveedores, distribuidores o terceros con acceso al sistema objetivo.

WEB THREATS: Amenazas que explotan vulnerabilidades en sitios web o navegadores.

ZERO DAY: Vulnerabilidad en SW, HW o FW desconocida por el proveedor y que aún no tiene un parche de seguridad.

Sectores objeto de ciberseguridad

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL



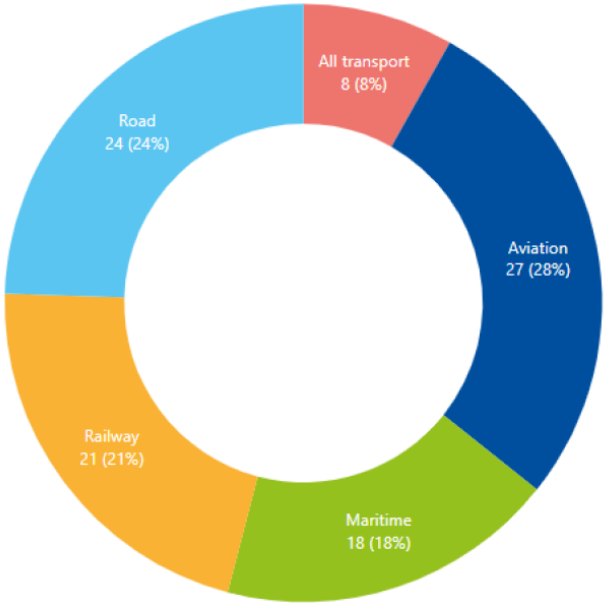
Fuente: 2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION
ENISA (EUROPEAN UNION AGENCY FOR CYBERSECURITY)

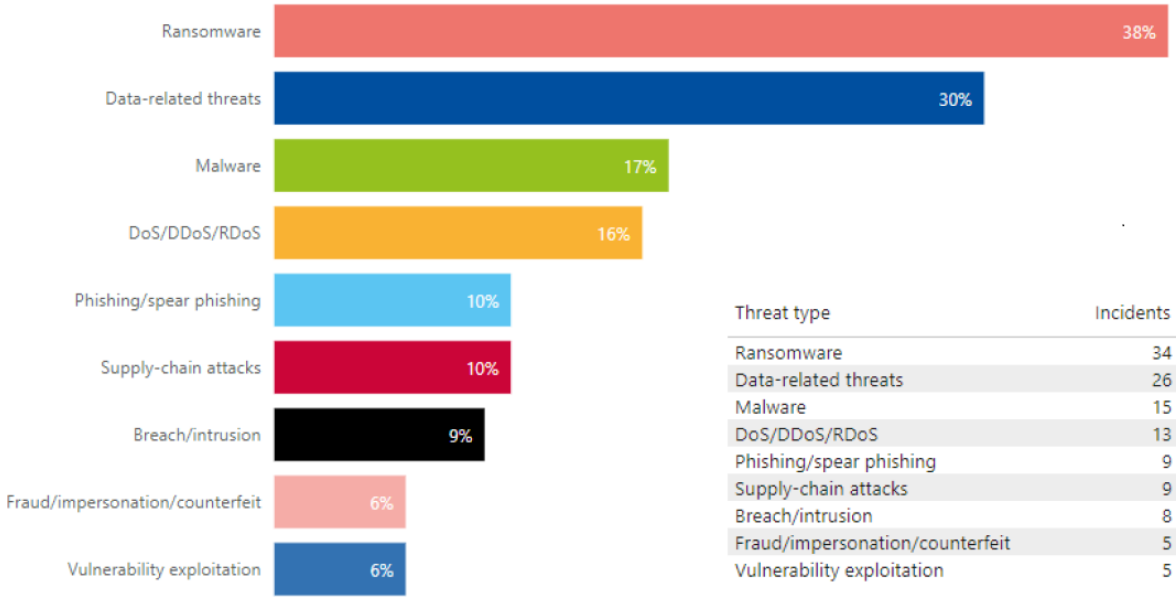
ENISA identifica el sector del Transporte como el segundo más afectado por eventos de ciberseguridad, con un 11% del total de ataques detectados entre Julio de 2023 y Junio de 2024.

Solo los organismos de la administración pública registraron un mayor número de incidentes.

Incidentes de ciberseguridad en sector Transporte

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL



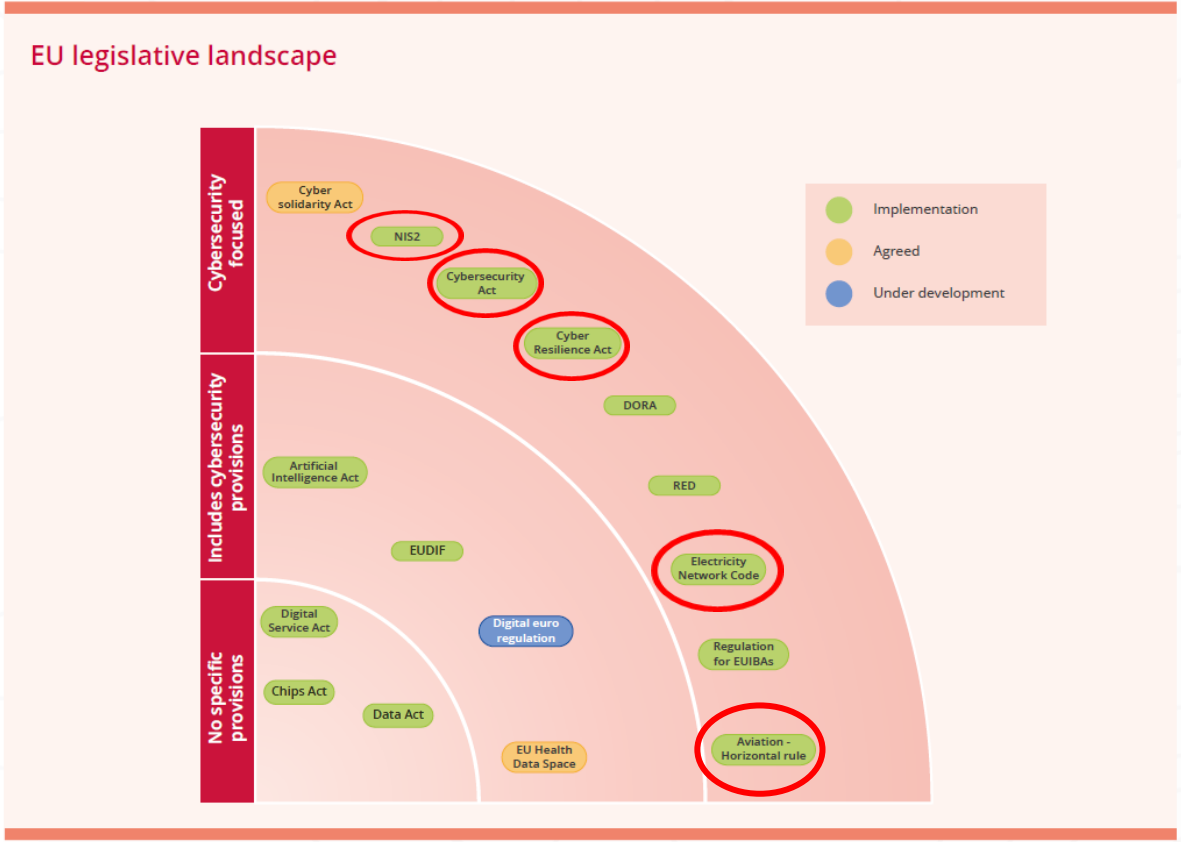


Threat type	Incidents
Ransomware	34
Data-related threats	26
Malware	15
DoS/DDoS/RDoS	13
Phishing/spear phishing	9
Supply-chain attacks	9
Breach/intrusion	8
Fraud/impersonation/counterfeit	5
Vulnerability exploitation	5

Fuente: ENISA THREAT LANDSCAPE: TRANSPORT SECTOR (January 2021 to October 2022)
ENISA (EUROPEAN UNION AGENCY FOR CYBERSECURITY)

Iniciativas legislativas en la UE en materia de ciberseguridad

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL



El marco legislativo de la UE en materia de ciberseguridad está en constante evolución y desarrollo.

Varias de estas iniciativas tendrán un impacto directo en el sector de Transporte.

NIS 2 y **CRA** serán las directivas con mayor impacto en este sector.

Fuente: 2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION ENISA (EUROPEAN UNION AGENCY FOR CYBERSECURITY)

íNDICE

Cyber Resilience Act: Objetivos y entidades afectadas

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- **TECNOLÓGICO**
- MEDIOAMBIENTAL
- **LEGAL**

CRA es un reglamento de la UE que establece requisitos obligatorios de ciberseguridad para productos con elementos digitales (HW y SW) vendidos en la UE.

Su objetivo es garantizar que estos productos sean seguros desde el diseño y durante todo su ciclo de vida.

Objetivos clave:

- Garantizar la seguridad desde el diseño (security by design).
- Exigir a los fabricantes actualizaciones de seguridad y gestión de vulnerabilidades.
- Reducir la exposición a ciberataques y riesgos de seguridad.
- Proteger a consumidores y empresas mediante estándares de ciberseguridad comunes en la UE.

¿A quién afecta?:

- Fabricantes, importadores y distribuidores de productos con componentes digitales (HW y SW)

Cyber Resilience Act: Obligaciones, sanciones y calendario

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL

CRA es un reglamento de la UE que establece requisitos obligatorios de ciberseguridad para productos con elementos digitales (HW y SW) vendidos en la UE.

Su objetivo es garantizar que estos productos sean seguros desde el diseño y durante todo su ciclo de vida.

Principales obligaciones:

- Ciberseguridad desde el diseño: Se tienen en cuenta en todas las fases del producto.
- Gestión de vulnerabilidades: Actualizaciones de seguridad durante todo el ciclo de vida del producto.
- Transparencia: Documentar los riesgos de ciberseguridad y dar información clara a los usuarios.
- Notificación de incidentes: Reportar vulnerabilidades e incidentes a ENISA y autoridades competentes.

Sanciones por incumplimiento:

- Multas de hasta 15 M€ o del 2.5% del volumen de negocio anual.

Calendario de entrada en vigor

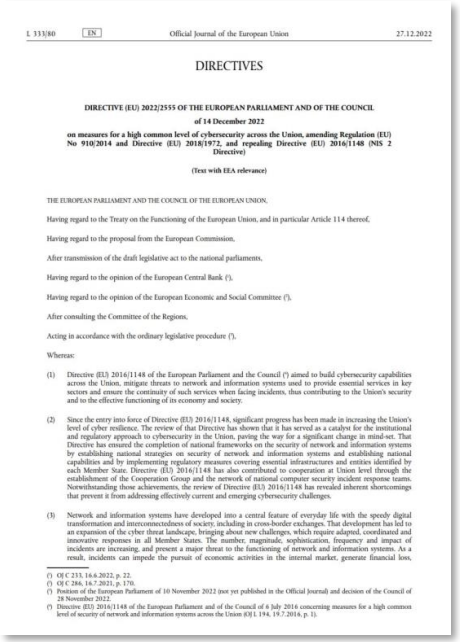
- 10 Diciembre 2024: Entrada en vigor oficial en todo el ámbito de la UE.
- 11 Septiembre 2026: Obligatoriedad de notificación de vulnerabilidades de ciberseguridad para fabricantes.
- 11 Diciembre 2027: Aplicación plena de las obligaciones del CRA en la UE (fabricantes tienen 3 años de período de adaptación).

NIS2 (Network & Information Security 2): Introducción

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL

La Directiva NIS2 (Directiva (UE) 2022/2555) es una disposición de la Unión Europea relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

Establece un marco regulatorio común de ciberseguridad, destinado a mejorar el nivel de ciberseguridad en la UE, exigiendo a los Estados miembros que fortalezcan sus capacidades de ciberseguridad, e introduciendo medidas de gestión riesgos de ciberseguridad y presentación de informes en sectores críticos, junto con normas sobre cooperación, intercambio de información, supervisión y aplicación.



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council (4) aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.

(2) Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss,

(1) OJ C 233, 16.6.2022, p. 22.
(2) OJ C 286, 16.7.2021, p. 170.
(3) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.
(4) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

NIS2. Información principal

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL

Eliminar las pronunciadas **diferencias** y **divergencias** en materia de ciberseguridad de los Estados Miembros

OBJETIVO

1

2

ESTABLECE

- Obligaciones de supervisión y ejecución para los Estados
- Medidas para gestion de riesgos
- Obligaciones de notificacion para las entidades
- Obligaciones intercambio de información sobre seguriad

NOVEDADES

3

- Seguridad cadena de suministro
- Relaciones con proveedores
- Responsabilidad alta de la dirección por incumpliminto de obligaciones.

4

APLICA A

- 20 Sectores
- Entidades públicas
- Entidades privadas

¿CUÁNDO?

Entra en vigor

2025

5

6

CUMPLIMIENTO

- Medidas técnicas
- Medidas de operación
- Medidas de organización

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL

NIS2. Sectores afectados

SECTORES DE ALTA CRITICIDAD

- Energía (electricidad, petróleo, gas, hidrógeno)
- **Transporte (aéreo, ferroviario, marítimo y fluvial, carretera)**
- Banca
- Infraestructuras de los mercados financieros
- Sector sanitario
- Agua potable
- Aguas residuales
- Infraestructura digital
- Gestión de servicios TIC
- Administración pública (excluidos el poder judicial, parlamentos y bancos centrales)
- Espacio
- Industria nuclear

OTROS SECTORES CRÍTICOS

- Servicios postales y mensajería
- Gestión de residuos
- Productos químicos
- Alimentación
- Industrias de fabricación
- Servicios digitales (marketplaces online, motores de búsqueda, redes sociales).
- Investigación
- Seguridad privada

NIS2. Entidades afectadas

IMPACTO:
- POLÍTICO
- **ECONÓMICO**
- **SOCIAL**
- TECNOLÓGICO
- MEDIOAMBIENTAL
- **LEGAL**

- Todas las entidades de cualquiera de los 20 sectores mencionados
- **Públicas y privadas**
- **Medianas o grandes empresas** (> 50 trabajadores o > 10 M€ de volumen anual de negocio)
- También afecta a pequeñas empresas cuando cumplen ciertas condiciones

- La directiva distingue entre **entidades esenciales e importantes**.
- (De forma simplificada) Se considera **entidad esencial** cualquiera que trabaje en los 12 sectores de alta criticidad (incluye **transporte**) y supere los límites de mediana empresa.
- Se considera entidad importante cualquiera que trabaje en cualquiera de los 20 sectores identificados en la directiva y que no tenga la consideración de esencial.

NIS2. Principales obligaciones

IMPACTO:
- POLÍTICO
- **ECONÓMICO**
- **SOCIAL**
- TECNOLÓGICO
- MEDIOAMBIENTAL
- **LEGAL**

- Aplica un régimen de supervisión por parte de las **autoridades** competentes, mediante **inspecciones y auditorías**
- Deber de **notificar los incidentes relevantes** de ciberseguridad al CSIRT o autoridad competente correspondiente (INCIBE y CCN, bajo coordinación del futuro CNC)
- Gestión de riesgos con proveedores y prestadores de servicios para garantizar la seguridad de la **cadena de suministro**
- Aumenta la **responsabilidad de los órganos de dirección**
- **Sanciones** de hasta 10 M€ o 2% del volumen de negocio anual para entidades esenciales.
- Adoptar **prácticas de ciberhigiene** como confianza cero, actualización de dispositivos, ...
- Adoptar **medidas técnicas, operativas y organizativas** para gestionar los riesgos y minimizar el impacto de incidentes
- Adoptar medidas de **gobernanza y gestión de riesgos** de ciberseguridad

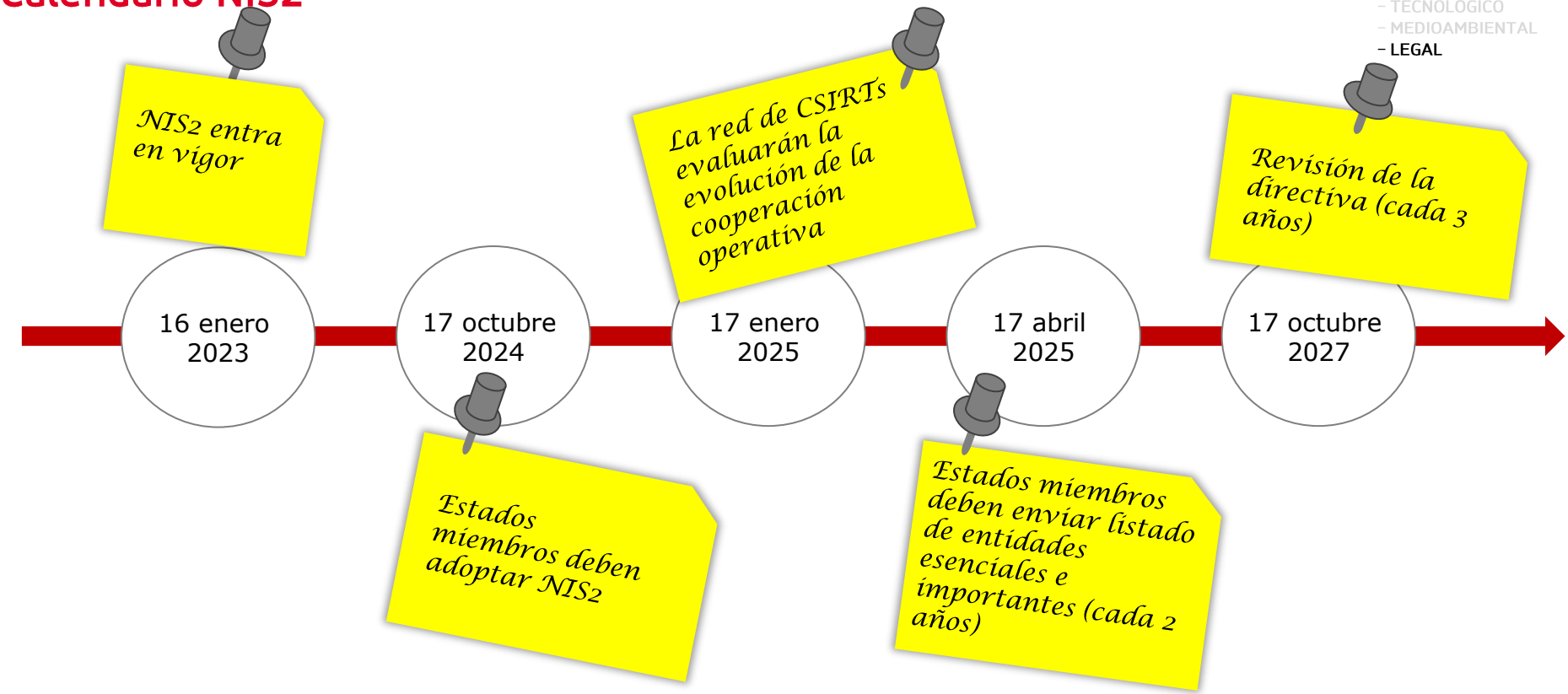
NIS2. Cadena de suministro

IMPACTO:
- POLÍTICO
- **ECONÓMICO**
- **SOCIAL**
- TECNOLÓGICO
- MEDIOAMBIENTAL
- **LEGAL**

- Una de las grandes novedades de NIS2 es la importancia que se concede a la **gestión de los riesgos de seguridad en la cadena de suministro**:
  - Proveedores de servicios de almacenamiento y tratamiento de datos.
  - Proveedores de servicios de seguridad gestionados.
  - Proveedores de Software.
  - Resto de proveedores con impacto en la prestación de servicio.
- Se debe incorporar en los **contratos con los proveedores y prestadores de servicio medidas para la gestión de todo tipo de riesgos con potencial impacto en el servicio.**
- Para ello, las empresas deben tener en cuenta la calidad y la resiliencia de los productos y servicios contratados, incluyendo la gestión de riesgos de ciberseguridad integrados en ellos, así como las **prácticas en materia de ciberseguridad y continuidad del negocio de sus proveedores y prestadores de servicio**, incluyendo las prácticas de desarrollo seguro.

IMPACTO:
- POLÍTICO
- ECONÓMICO
- SOCIAL
- TECNOLÓGICO
- MEDIOAMBIENTAL
- LEGAL

Calendario NIS2



Muchas gracias

ahernandez@gmv.com